2017 AFP

Payments Fraud and Control Survey

REPORT OF SURVEY RESULTS

AFP® ASSOCIATION FOR FINANCIAL PROFESSIONALS

Underwritten by

J.P.Morgan

2017 AFP Payments Fraud and Control Survey

REPORT OF SURVEY RESULTS

March 2017

Underwritten by

J.P.Morgan

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Association for Financial Professionals
4520 East-West Highway, Suite 750
Bethesda, MD 20814
Phone 301.907.2862
Fax 301.907.2864
www.AFPonline.org

J.P.Morgan

For the ninth consecutive year, J.P. Morgan is proud to once again sponsor the AFP Payments Fraud and Control Survey, and we're pleased to provide you with this copy of AFP's 2017 report.

This year's survey results demonstrate that cybersecurity models and strict control governance are crucial for all businesses, given that 75 percent of companies were targets of payments fraud last year. Additionally, the survey reveals that:

- 75 percent of organizations experienced check fraud in 2016. This is an increase from 71 percent in 2015 and a reversal of the declining trend in check fraud since 2010.
- 74 percent reported that their organizations were exposed to business email compromise (BEC), a 10 percent increase from the prior year.
- Over 70 percent of corporate treasury and finance professionals are hesitant about adopting mobile payments at their organizations, as they question the security of this payment method.
- Nearly half of survey respondents reported that the incidents of fraud attempts increased in 2016.

With these statistics in mind, it's important for all businesses to take preventive measures to protect their payments, including educating their employees on current payments fraud practices, and implementing the products and processes they need to protect their 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're committed to fraud mitigation and information protection across our entire infrastructure, and we'll 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'd like to thank the AFP for providing us with this year's valuable insights—they are a cautious reminder that the best defense is to remain vigilant in fraud detection and cybersecurity protection protocols.

With best regards,

Nancy K. McDonnell
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 has been a concern for organizations for many years, but has become an even more troublesome issue recently. While enterprising criminals keep developing new and innovative ways of scamming their victims, they are also reverting back to old-fashioned methods, such as check fraud. In the United States, checks are the payment method most often subject to fraud, likely due to the extensive use of checks for business-to-business (B2B) transactions.

In addition, new technology is providing fraudsters with an expanding set of tools to commit fraud—particularly with checks—and is also enabling them to develop new forms of fraud, such as business email compromise (BEC) scams. Since all organizations, to some extent, make financial transactions, they consequently are also potential targets for these criminals. One of the toughest challenges for corporations is that these technologically savvy individuals seem to be at least one step ahead of organizations' methods to guard against fraud. It usually takes some time before information on how to protect against new fraud approaches reaches potential targets, and so the scams can continue for a while. It is impossible for organizations to be completely protected from payments fraud, but there is much they can do to limit their exposure to it.

Each year since 2005, the Association for Financial Professionals® (AFP) has conducted its *Payments Fraud and Control Survey* to examine the trends in payments fraud in business-to-business (B2B) activities, the level of fraud activity, payment methods impacted by fraud and the extent of the impact from fraud. The survey also captures information on the strategies and controls being implemented by organizations, and highlights the emergence of any new tactics fraudsters are adopting.

Continuing these efforts, in January 2017 AFP conducted its 13th Annual *Payments Fraud and Control Survey*. The survey generated 547 responses from corporate practitioners from organizations of varying sizes, representing numerous industries. Their responses form the basis of this report and reflect data for 2016.

AFP thanks J.P. Morgan for its underwriting support of the *2017 AFP Payments Fraud and Control Survey*. Both the questionnaire design and the final report are the sole responsibility of AFP's Research Department. Information on the demographics of the respondents can be found at the end of the report.

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Payments Fraud Overview

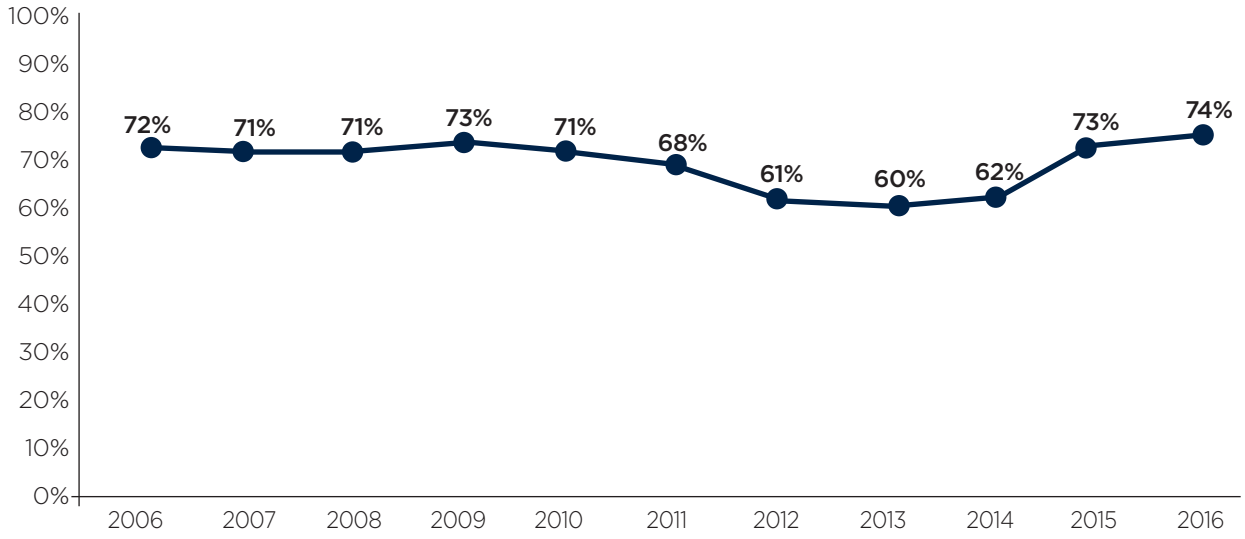
After a gradual decline in the percentage of organizations that experienced attempted or actual payments fraud from 2009 to 2013, there was an uptick in the share of companies that were victims of payments fraud attempts and attacks. In 2015, 73 percent of organizations were targets of payments fraud—a significant increase of 11 percentage points from 2014.

That upward trend continued; 74 percent of finance professionals report that their companies were victims of payments fraud in 2016. This is the largest share on record, exceeding the previous record-high share of 73 percent in both 2009 and 2015, and significantly higher than the percentages reported between 2011 and 2014. It suggests that fraudsters are continuing to succeed in their attempts to attack organizations' payment systems.

The fact that overall payments fraud is currently at its highest level is troubling. It signals that organizations cannot be complacent about the threats of payments fraud. All organizations can certainly be targets of fraud, and it is important for them to take the necessary steps to make it as difficult as possible for criminals to succeed in their attacks.

74% of organizations were victims of payments fraud in 2016

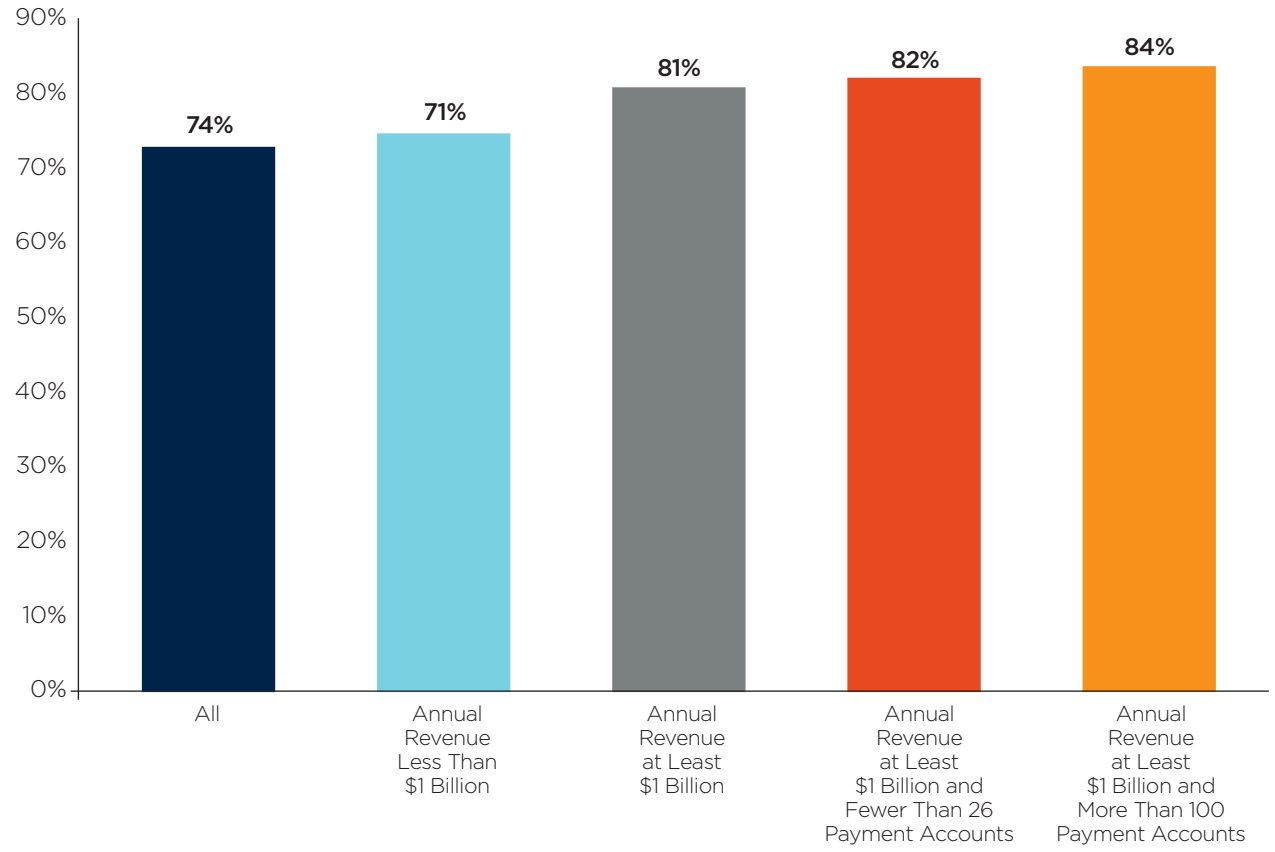
Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2006-2016



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Organization size appears to have had an impact on the incidence of payments fraud in 2016. Those organizations with at least $1 billion in annual revenue were more likely to have been subject to fraud than were smaller organizations with annual revenue of less than $1 billion.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2016



Checks continue to be the payment method most frequently targeted by those committing or attempting to commit fraud. Seventy-five percent of organizations that were victims of fraud attempts/attacks in 2016 experienced check fraud. This is an increase from the 71 percent that experienced check fraud in 2015.

The fact that check fraud remains the most prevalent form of payments fraud is not surprising. Checks continue to be the payment *method* most often used by organizations. According to the *2016 AFP Electronic Payments Survey*, 51 percent of companies' B2B payments are made by check. Since checks are more prevalent as a payment method, they subsequently are most often targets of fraud. Another possible reason for the increase in payments fraud via check could be business email compromise (BEC) scams that target checks to some extent.

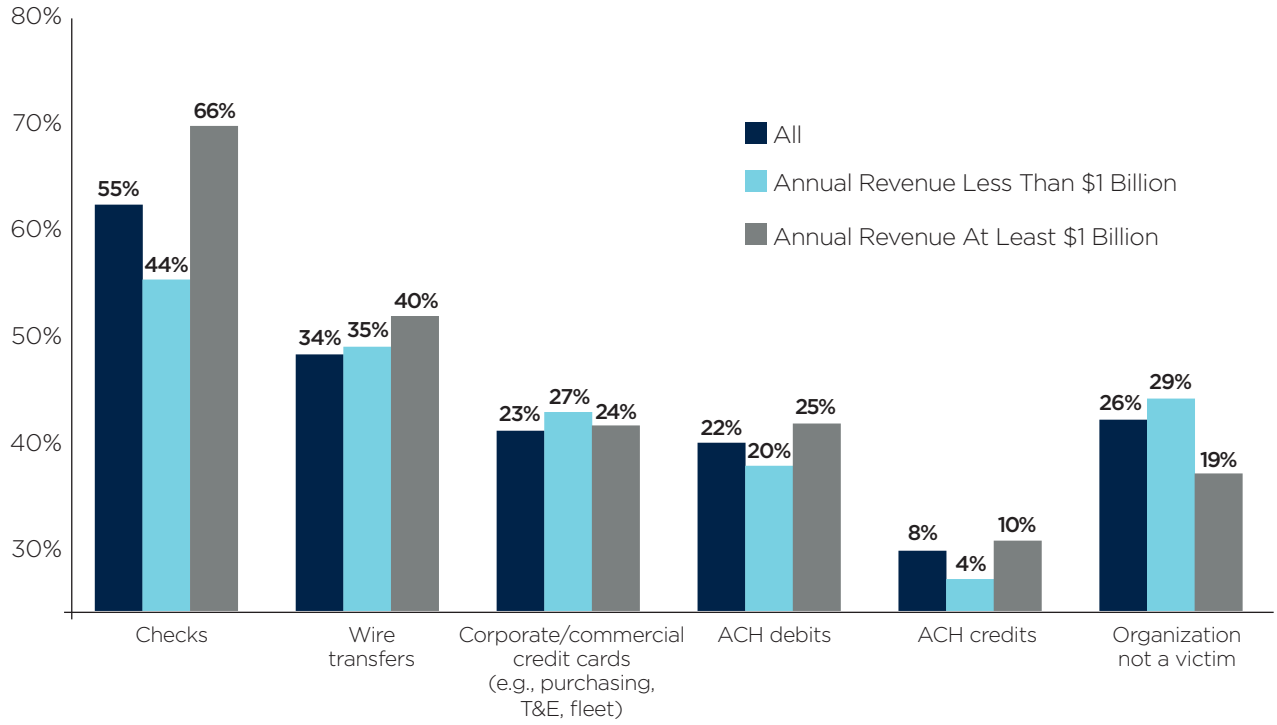
Checks continue to be the payment method most often exposed to fraud activity

©2017 Association for Financial Professionals, Inc. All Rights Reserved

In 2016, wire transfers were the second most-often targeted payment method attacked by fraudsters. Forty-six percent of corporate practitioners whose organizations had experienced attempted or actual payments fraud report that such attacks were via wire transfers. This is similar to the 48 percent of finance professionals who reported wire transfer fraud in 2015, but a significant increase from the 27 percent and 14 percent who reported wire transfer fraud in 2014 and 2013, respectively.

Wire transfers were the 2nd most-often targeted payment method in 2016

Payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2016*
(Percent of Organizations)



This chart also includes data for organizations that had not experienced attempted/actual fraud

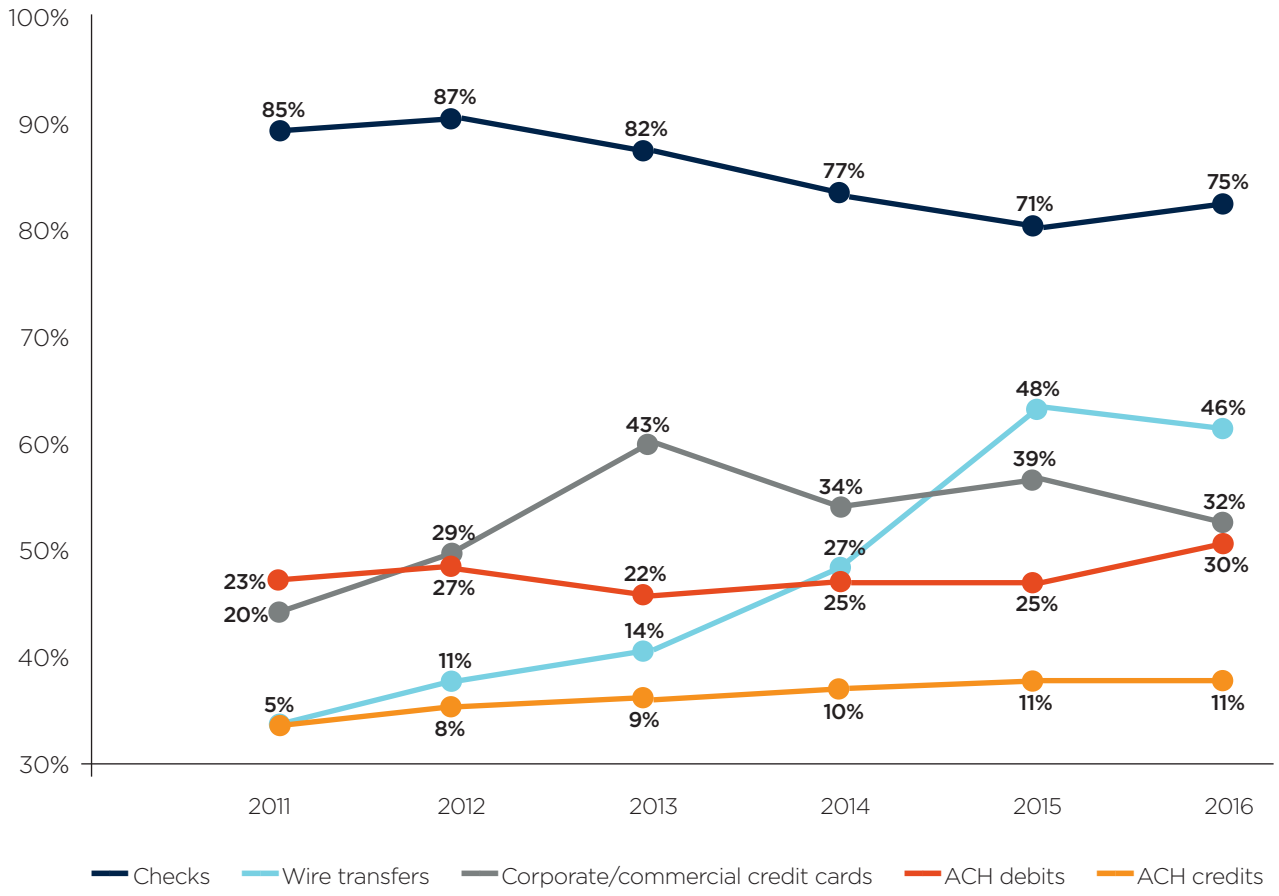
Finance professionals are increasingly dealing with business email compromise (BEC) scams. (More information about BEC is covered later in this report.) While checks are often targets of BEC scams, the main target—or preferred payment method—for BEC scams remains wire transfers. Looking at the long-term trends in wire fraud, it is evident that the share of organizations subject to payments fraud via wire transfers has increased dramatically. Only five percent of finance professionals reported wire fraud in 2009, but the share rose continually—and dramatically—peaking at 48 percent in 2015. The dramatic increase in wire fraud coincided directly with the rise in BEC scams. The fact that wire fraud is still being reported around a similarly elevated level (46 percent) indicates that BEC scams—unfortunately—continue to be prevalent and effective.

Fraud via corporate/commercial credit cards accounted for the third largest share of fraud (cited by 32 percent of survey respondents), followed closely by ACH debits (30 percent) and ACH credits (11 percent). The incidence of payment fraud via cards has experienced significant upward and downward movements. Card fraud peaked in 2013 at 43 percent, likely due to large data breaches at major retailers in which card credentials were stolen.

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Also noteworthy is the recent rise in ACH debit fraud—from 25 percent in both 2014 and 2015 to 30 percent in 2016. The 2016 figure is higher than in any of the previous years' surveys, and could be an indication of some new type of fraud. As always, it is vital that finance professionals stay alert and report instances of fraud to authorities.

Trends in Payments Fraud Activity
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



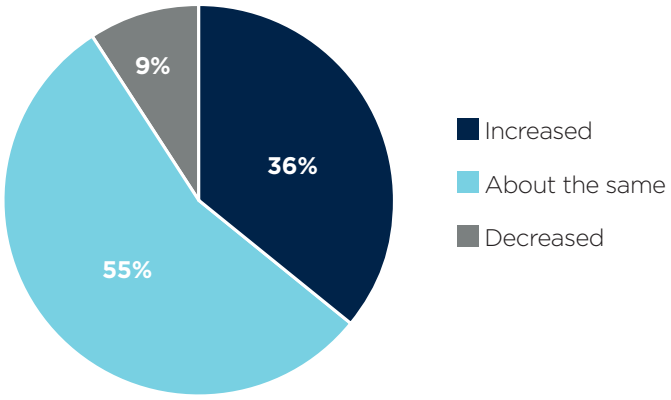
A majority of finance professionals (55 percent) reports that the incidence of payments fraud at their companies in 2016 was unchanged from 2015. Thirty-six percent of respondents whose organizations experienced payments fraud report that the number of incidents of fraud attempts increased in 2016 compared to 2015 and nine percent indicate it had decreased. These results reflect a slight improvement from the previous year when 42 percent of survey respondents indicated the incidence of payments fraud increased in 2015 compared to 2014. Larger organizations with annual revenue of at least $1 billion were more likely than smaller companies to have experienced an increase in fraud activity over the past year (42 percent in 2016 versus 35 percent in 2015).

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Protecting themselves from payments fraud can be very difficult for organizations. Certainly there are a number of products in the market that can help fight fraud on some level. However, criminals are relentless and are constantly discovering new ways to infiltrate organizations; most companies simply do not have the resources to adequately protect themselves. Their banking partners can provide a number of protective measures such as positive pay, etc. But those measures come with a cost, and those costs can directly affect an organization's bottom line.

Another challenge is how different businesses handle EMV technology. For big-ticket-item retailers, EMV makes more sense than for retailers in a high-volume, low-value business such as fast food restaurants. The cost of investing in new EMV-enabled terminals (which authenticate chip card transactions) for fast-food restaurants is significant, and those businesses may not be experiencing considerable fraud. There are cases where certain businesses will risk payments fraud merely because a financial loss incurred from a fraud attack may be lower than the cost of investing in new terminals.

Change in Incidence of Payments Fraud in 2016 Compared to 2015
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Financial Loss from Fraud Attempts

A majority of companies that were targets of payment fraud in 2016 suffered a relatively small financial loss as a result. Fourteen percent of organizations that experienced payments fraud in 2016 did not have a financial loss from the fraud. For 25 percent of those that did, the potential loss from fraud in 2016 was estimated at less than $25,000; for 32 percent of them the loss was between $25,000 and $249,999. The potential loss was estimated at $250,000 or more at 29 percent of organizations.

Larger organizations with annual revenue greater than $1 billion were more likely than other companies to have experienced potential financial loss in the higher dollar ranges. Thirty-nine percent of corporate practitioners from these companies report the potential loss from fraud in 2016 was greater than $250,000. Notably, 32 percent of finance professionals from larger organizations with more than 100 payment accounts report the potential fraud loss in 2016 was more than $500,000.

Potential Financial Loss from Attempted or Actual Payments Fraud in 2016
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)

	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
No Loss	14%	20%	9%	11%	8%
Up to $24,999	25	28	20	27	16
$25,000-$49,999	9	9	10	11	8
$50,000-$99,999	11	13	9	8	8
$100,000-$249,999	12	14	12	13	16
$250,000-$499,999	10	6	13	13	12
$500,000-$999,999	4	2	5	4	12
$1,000,000-$1,999,999	7	5	8	6	4
Over $2,000,000	8	4	13	8	16

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Seventy-five percent of organizations that were exposed to at least one payments fraud attempt in 2016 did not incur an *actual* financial loss from that attempt. Thirteen percent of survey respondents report a financial loss to their organizations of less than $25,000 due to payments fraud, and only four percent report a loss greater than $250,000. Over one-third of larger organizations maintaining more than 100 payment accounts were likely to experience a direct financial loss due to payments fraud.

Actual Direct Financial Loss from Attempted and/or Actual Payments Fraud in 2016
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)

	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
No Loss	75%	82%	71%	75%	65%
Up to $24,999	13	13	11	16	4
$25,000-$49,999	3	–	4	1	4
$50,000-$99,999	4	3	5	2	12
$100,000-$249,999	3	1	5	3	12
$250,000-$499,999	1	–	1	1	–
$500,000-$999,999	1	1	–	–	–
$1,000,000-$1,999,999	1	–	2	1	4
Over $2,000,000	1	–	1	–	–

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Costs to manage/defend and/or clean up from fraud attacks were relatively low for most organizations. Forty-eight percent did not incur any expenses due to a fraud attempt, and 41 percent spent less than $25,000 to defend against or clean up the fraud. A greater share of larger organizations—specifically those with more payment accounts—were more likely to have spent more on cleaning up and defending against fraud than were other companies.

Cost to Manage/Defend/Cleanup from Attempted and/or Actual Payments Fraud in 2016
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)

	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
No Cost	48%	59%	38%	43%	26%
Up to $24,999	41	37	46	49	39
$25,000-$49,999	4	3	4	1	9
$50,000-$99,999	2	1	3	2	4
$100,000-$249,999	4	–	6	3	22
$250,000-$499,999	1	–	2	1	–
$500,000-$999,999	–	–	–	–	–
$1,000,000-$1,999,999	–	–	–	–	–
Over $2,000,000	–	–	–	–	–

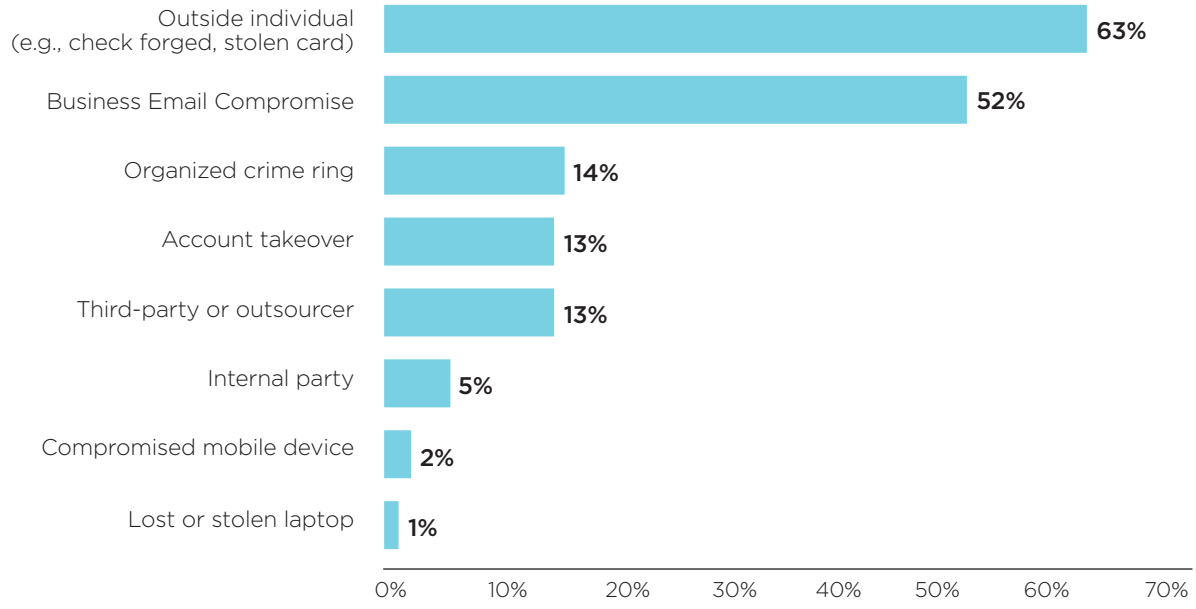
©2017 Association for Financial Professionals, Inc. All Rights Reserved

Sources of Attempted/Actual Payments Fraud

The majority of payments fraud continues to originate from an external source or individual. Almost two-thirds of companies (63 percent) that experienced attempted or actual payments fraud in 2016 did so as a result of actions by an outside individual. Fifty-two percent of finance professionals report that at their companies, payments fraud originated via business email compromise (BEC) while 14 percent were targets of an organized crime ring.

The majority of payments fraud continues to originate from an **external source** or **individual**

Sources of Attempted/Actual Payments Fraud in 2016
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Business Email Compromise (BEC)

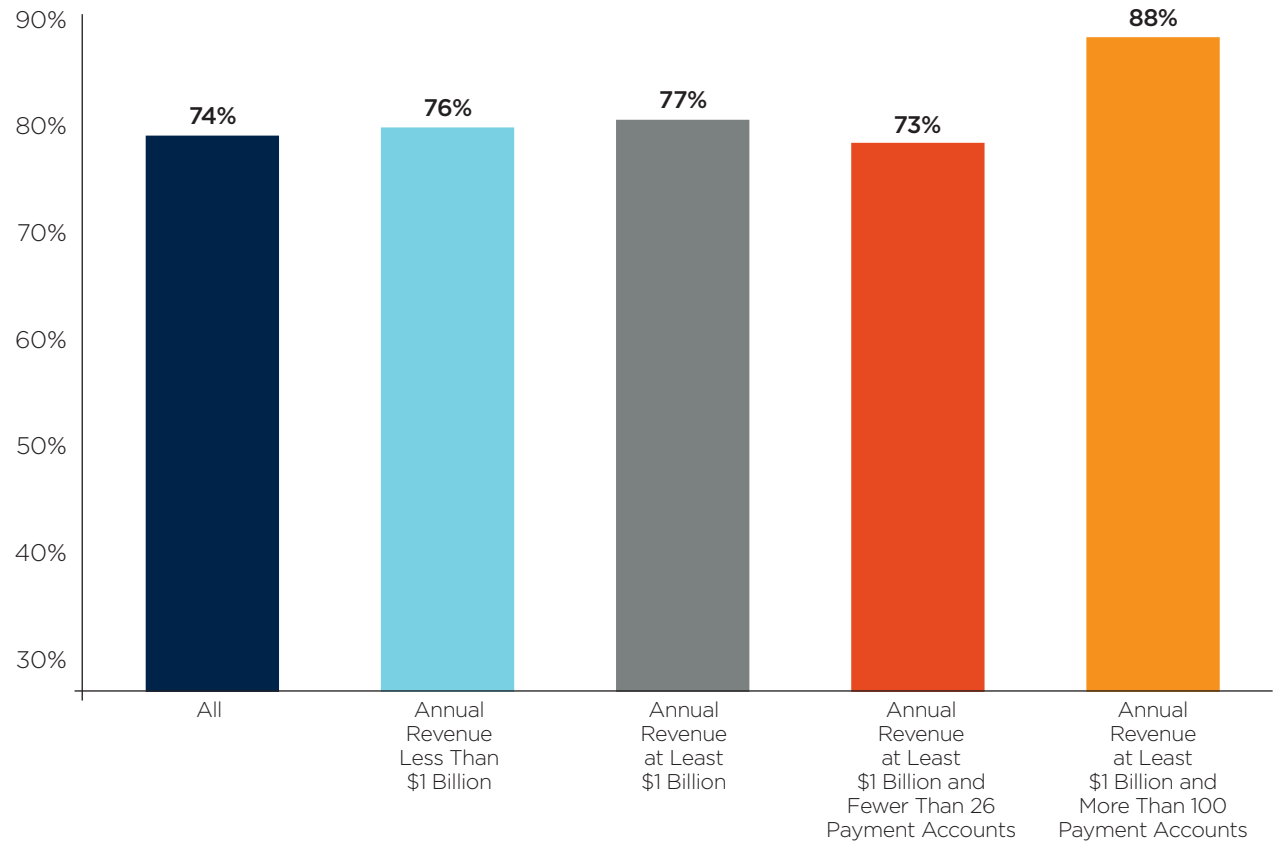
The past few years have seen a sharp uptick in business email compromise (BEC) scams. A **2016 FBI alert** defines BEC as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds." While these scams target wire payments for the most part, they also target checks to a significant extent. With overall payments fraud at similarly elevated levels in both 2015 and 2016, it certainly appears that these scams are effective.

The FBI alert also indicates that BEC scams are increasing, evolving and targeting businesses regardless of size or geographic location. The FBI has received reports of BEC scams from organizations in all 50 states and 100 countries, and losses from such scams have increased exponentially since January 2015. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to banks in China and Hong Kong.

Fully 74 percent of finance professionals report that their organizations were victims of BEC in 2016. This is a 10-percentage point increase from 2015. BEC was more prevalent among larger organizations with annual revenue of at least $1 billion and more than 100 payment accounts than similarly sized organizations with fewer than 26 payment accounts.

Nearly **three-fourths** of companies were **victims of business email compromise** in 2016

Percent of Organizations that Experienced Attempted and/or Actual Business Email Compromise in 2016



©2017 Association for Financial Professionals, Inc. All Rights Reserved

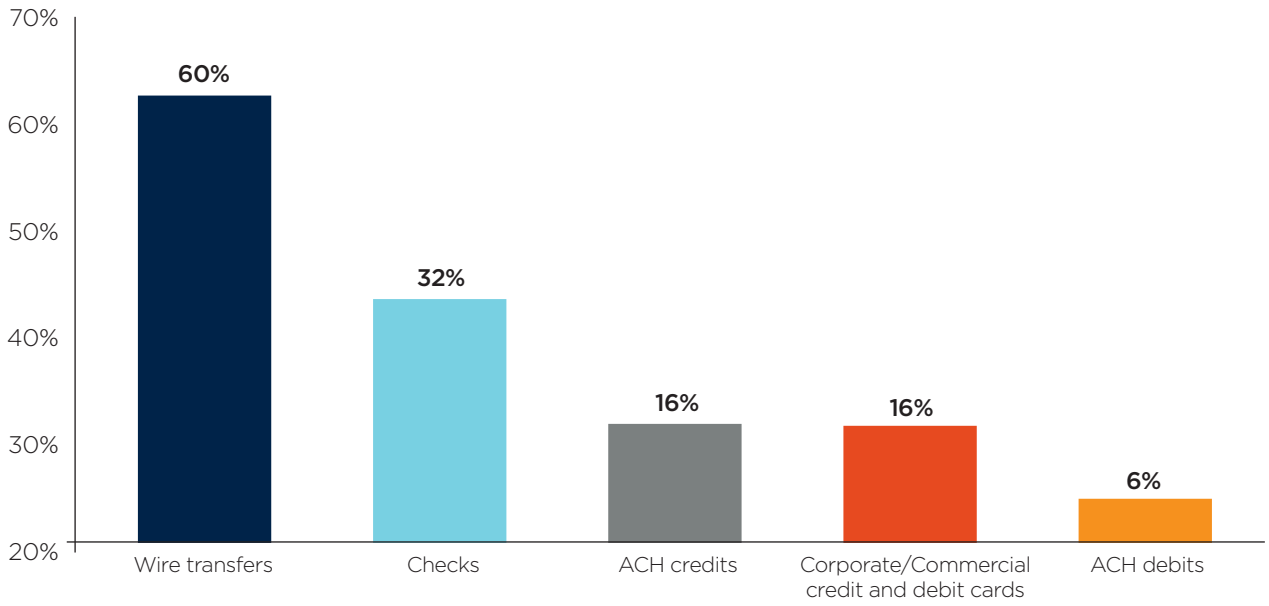
When BEC scams first started occurring, it took many finance professionals by surprise. What looked like a regular email from a CEO or CFO requesting the accounts payable department to make a quick transfer for a merger or other important transaction appeared authentic, and so the payment was made. Fraudsters were successfully using email, a vehicle extensively used in business communications, to steal from unsuspecting targets.

It should be fairly simple to guard against BEC scams, and solid internal controls are key to doing so. Every organization needs to have policies in place to prevent funds transactions being initiated by an email. The finance team and senior management need to communicate with employees regarding BEC, explain what to look out for, and always encourage staff to check before taking any action regarding a payment, such as implementing dual authentication—that is, transactions should not be authorized without a second signature. Given the broad spectrum of BEC scams, it is also important to plan for scenarios such as changes in payment information with external providers, etc. In many cases a simple call to a trusted phone number on file will ensure that information is authentic.

Sixty percent of organizations that experienced actual payments fraud via BEC did so via wire transfers. That result is a slight increase from the 56 percent in 2015. Although nearly three quarters of organizations were subject to BEC, fortunately less than half (47 percent) incurred a financial loss as a result.

60% of companies that experienced payments fraud via business email compromise did so via **wire transfers**

Payment Methods Impacted by Actual Loss as a Result of Business Email Compromise (BEC)
(Percent of Organizations that Experienced Financial Loss Due to BEC)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Estimated Total Dollar Amount of the Potential and Actual Financial Loss Resulting from Business Email Compromise (BEC) in 2016
(Percentage Distribution of Organizations that Experienced Payments Fraud via BEC)

	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
No Loss	53%	58%	47%	49%	30%
Up to $24,999	11	15	10	13	9
$25,000-$49,999	4	5	4	6	–
$50,000-$99,999	6	7	5	3	13
$100,000-$249,999	9	9	10	9	22
$250,000-$499,999	6	3	7	9	9
$500,000-$999,999	3	–	3	1	4
$1,000,000-$1,999,999	4	3	6	4	9
Over $2,000,000	5	1	8	6	4

A vast majority of corporate practitioners reports that their organizations are being proactive in preventing BEC, and have either implemented controls to guard against being impacted from BEC (71 percent) or are in the process of determining the controls that need to be in place to protect their organizations from BEC (10 percent). Another 12 percent are considering implementing controls. Eight percent do not believe there is a need. Over 90 percent of larger organizations with more than 100 payment accounts have controls in place to prevent being impacted by BEC.

81% of organizations have either implemented or are in the process of implementing controls to guard against business email compromise

Implemented New Controls to Prevent Business Email Compromise
(Percentage Distribution of Organizations)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes, have implemented several new internal controls to prevent being impacted by BEC	71%	61%	79%	74%	92%
Yes, are in the process of determining the controls that should be in place to prevent BEC	10	14	6	8	4
Not yet, but are considering it	12	15	9	12	–
No, do not see the need	8	11	6	6	4

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Check Fraud

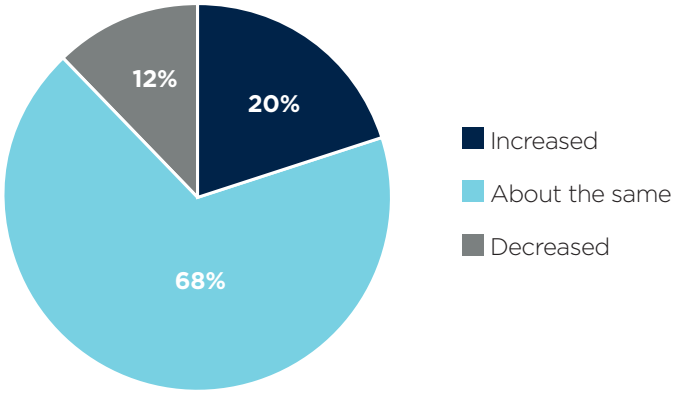
Checks have been and continue to be the payment method most often exposed to fraud activity. Fifty-nine percent of organizations that experienced check fraud in 2016 suffered between one and five incidents; 15 percent were subject to between six and 10 incidents and 16 percent were exposed to 21 or more instances. Larger organizations with annual revenue of at least $1 billion were far more likely than other companies to have been victims of check fraud. Thirty-one percent of survey respondents from this group report their organizations experienced check fraud more than 15 times in 2016.

Number of Times Organization Experienced Attempted and/or Actual Check Fraud in 2016
(Percentage Distribution of Organizations that Experienced At Least One Attempt of Check Fraud)

	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
1-5	59%	72%	45%	49%	45%
6-10	15	12	18	17	10
11-15	5	3	7	5	14
16-20	5	5	6	8	7
21-more	16	8	25	21	24

Over two-thirds (68 percent) of finance professionals report that the number of check fraud attempts at their organizations was unchanged from that in 2015, while 20 percent report an increase.

Change in Incidence of Check Fraud in 2016 Compared to 2015
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud via Checks)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Positive pay continues to be the method most often used by organizations to guard against check fraud, used by 74 percent of organizations. Other methods include:

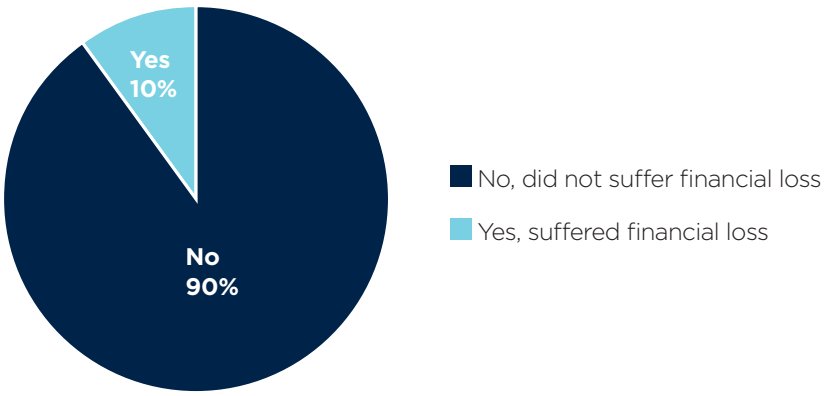
- Segregation of accounts (cited by 69 percent of respondents)
- Daily reconciliations and other internal processes (64 percent)
- Payee positive pay (41 percent).

Fraud Control Procedures Used to Guard against Check Fraud
(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)

	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
Positive pay	74%	71%	82%	85%	100%
Segregation of accounts	69	57	86	84	50
Daily reconciliation and other internal processes	64	57	64	77	–
Payee positive pay	41	29	55	54	50
"Post no checks" restriction on depository accounts	38	21	55	77	–
Reverse positive pay	13	14	14	15	50
Non-bank fraud control services	10	–	14	15	–

Although 55 percent of organizations experienced check fraud in 2016, only 10 percent of companies suffered a financial loss as a result. Indeed, the vast majority did not experience a financial loss as a consequence. Lack of positive pay (cited by 23 percent of respondents) and clerical errors (18 percent) were two primary reasons for financial loss due to check fraud.

Organization Suffered Financial Loss as a Result of Check Fraud
(Percentage Distribution of Organizations that Experienced At Least One Attempt of Check Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Finance professionals are eager to mitigate the instances of check fraud and are cognizant of the fact that certain security features are more effective in preventing it. Fifty-nine percent of survey respondents consider the VOID feature (the word "VOID" appears if check is scanned or copied) effective in preventing fraud. Other features cited by respondents as being effective in include a dual-tone true watermark (cited by 36 percent of respondents) and microprint (a fine line of print that is difficult to photocopy and can only be read when magnified (35 percent). Other features considered effective in preventing check fraud are customized controlled paper stock, chemical wash detection box, chemical reactive paper and thermochromatic ink.

Positive pay is a well-established and very effective protective measure. By matching a list of issued checks from a client organization with those it presents for payment, a bank can determine discrepancies and send them back to the issuer. Thus, positive pay not only detects fraudulent doubles but also other alterations to checks. Daily reconciliation is also an effective protective measure but can be quite cumbersome. So setting aside resources for such efforts can be a good investment.

Security Features Most Effective in Preventing Check Fraud
(Percentage Distribution of Organizations that Experienced Payments Fraud via Checks)

	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
VOID Feature (The word "VOID" appears if check is scanned or copied)	59%	62%	59%	65%	37%
Dual-tone true watermark	36	43	31	31	37
Micro print (a fine line of print can be read when magnified—difficult to photocopy)	35	43	31	29	33
Customized controlled paper stock (not available in the marketplace)	26	25	27	30	7
Chemical wash detection box (deters check washing by warning forgers that fraud will be evident)	22	23	23	19	23
Chemical reactive paper (causes the check to stain from ink eradicator chemicals)	22	21	23	28	10
Thermochromatic ink (reacts to changes in temperature)	21	21	19	19	13
Warning banners (calls attention to the safety features in the check)	19	23	16	19	10
High resolution border with chemically reactive ink that dissolves in acetone	15	16	16	18	7
Fluorescent fibers	8	6	10	10	13
Fluorescent ink	7	5	8	9	10

©2017 Association for Financial Professionals, Inc. All Rights Reserved

ACH Fraud

ACH transactions have some advantages over check payments. One advantage is that they are considered more secure than checks and therefore require more of an effort for criminals to be successful in committing fraud via ACH. ACH transactions are often generated through large files sent from organizations to their banks. Those are much more difficult to compromise than merely altering credentials or features on paper checks. In order to commit successful ACH fraud, criminals may even have to partner with individuals inside the targeted organization in order to bypass any security features in place.

Despite this, the incidence of ACH debit fraud increased in the past year. At the same time, fraud via ACH credit has remained at a fairly low level. Any increase in fraud means that something is not working the way it should, or criminals have come up with new scams that bypass current security.

In 2016, 30 percent of organizations were subject to ACH debit fraud and 11 percent to ACH credit fraud. Larger organizations with more than 100 payment accounts were six times more likely to have experienced more than 20 attempts of payments fraud via ACH than were similarly sized organizations with fewer payment accounts. Eighty-four percent of organizations were exposed to between one and five ACH fraud incidents. Only five percent of finance professionals report their organizations were subject to more than 20 incidents of ACH fraud.

Number of Organizations that Experienced Attempted and/or Actual ACH Fraud in 2016
(Percentage Distribution of Organizations that Experienced At Least One Attempt of ACH Fraud)

	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
1-5	84%	90%	77%	85%	59%
6-10	6	4	7	3	15
11-15	3	1	6	5	4
16-20	2	1	3	3	4
21-more	5	4	7	3	19

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Eighty percent of corporate practitioners report that the number of instances of ACH fraud attempts at their organizations in 2016 was unchanged from that in 2015. Thirteen percent report a rise in incidents of ACH fraud during the same timeframe and only seven percent report a decrease.

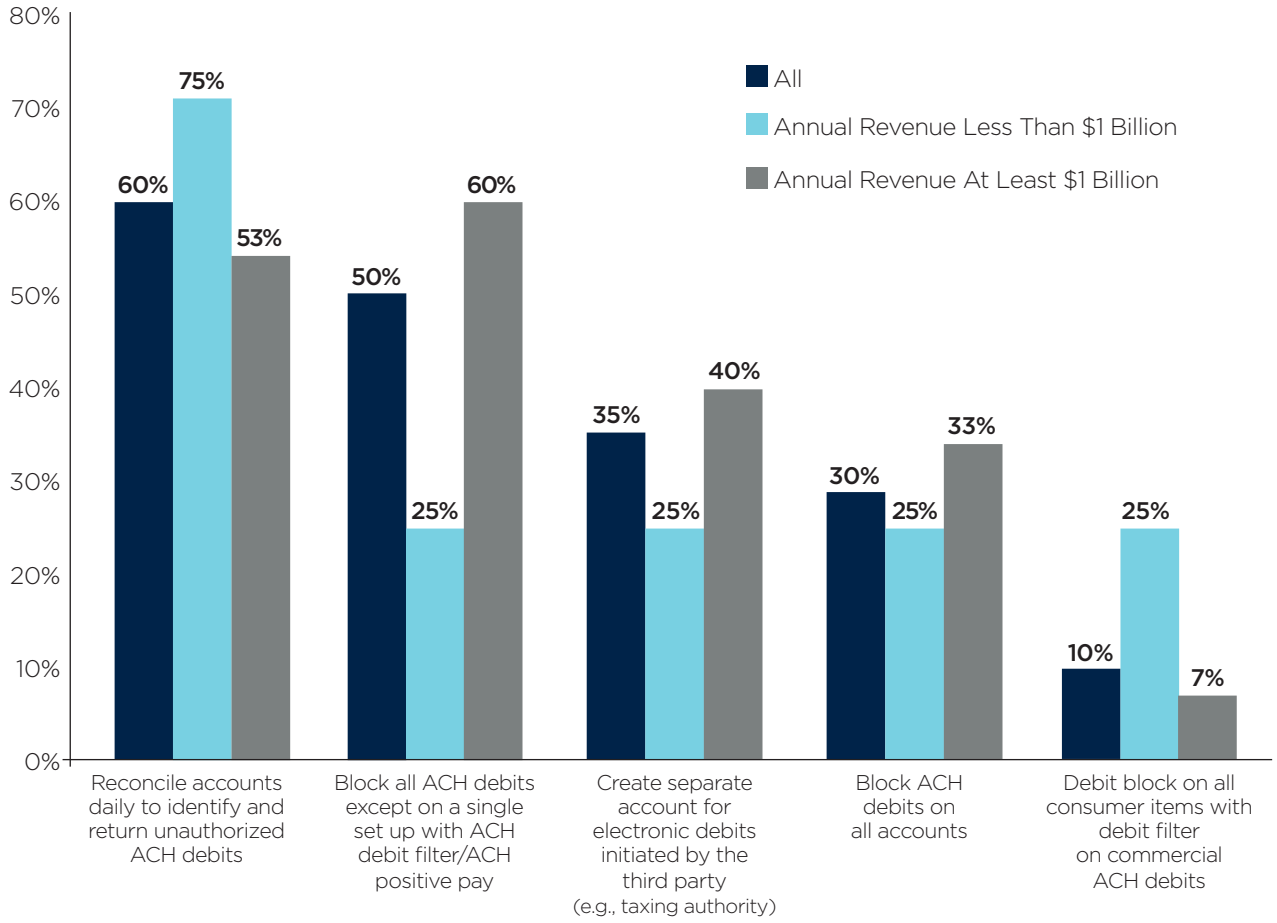
Only five percent of finance professionals indicate their organizations suffered a financial loss as a result of ACH fraud. This share increased to 16 percent for larger organizations with more than 100 payment accounts.

The primary reasons for ACH fraud include:

- **ACH return not timely** (cited by 33 percent of respondents)
- **Gaps in online security controls/criminal account takeover** (29 percent)
- **Did not use ACH debit blocks or ACH credit filters** (24 percent)

Organizations implement various tactics to reduce the impact of ACH fraud. Sixty percent of companies reconcile accounts daily to identify and return unauthorized ACH debits, while 50 percent block all ACH debits except on a single account set-up with ACH debit filters/ ACH positive pay. Thirty-five percent create separate accounts for electronic debits initiated by a third party and 30 percent block ACH debits on all accounts.

Fraud Control Procedures Used to Prevent ACH Fraud
(Percent of Organizations that Experienced At Least One Attempt of ACH Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Corporate/Commercial Card Payments

The use of commercial cards has undergone some turbulence in the last couple of years. In 2013, before the highly publicized data breaches at major retailers, card use for corporate transactions had increased significantly. There are a number of reasons why. Cards can be a very convenient payment method to use; an organization can simply issue commercial cards to employees, and the use of cards can be restricted to pay only for certain things or have limited spending amounts. However, after the retail breaches, commercial card use declined abruptly, as has been reported in previous *AFP Payments Fraud and Control Surveys*. Since then, the use of certain cards, such as purchasing cards, has again started to increase, but not to the extent seen prior to the breaches. Despite the convenience of using cards, there is still some concern regarding loss of card credentials but to a much lesser extent in 2016 than in 2013. As time passes, the memory of the impact from large computer data breaches fades away.

The most widely used corporate/commercial cards for B2B transactions in 2016 continued to be purchasing cards, used by 73 percent of organizations (slightly less than the 75 percent reported in 2015), followed by Travel & Entertainment (T&E) cards (46 percent, similar to 45 percent in 2015). Thirty-one percent of companies used ghost and virtual cards (29 percent in 2015). Larger organizations with more than 100 payment accounts were more likely to have used ghost or virtual cards and T&E cards than were other organizations.

Purchasing cards are the most widely used corporate/commercial cards for B2B transactions

Percentage of Corporate/Commercial Cards that Organizations Use for B2B Payments
(Percent of Organizations that Experienced Attempted and/or Actual Fraud via Corporate/Commercial Cards)

	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
Purchasing cards	73%	65%	82%	82%	82%
T&E cards	46	44	51	48	61
Ghost or virtual cards (valid card account without a physical card issued)	31	26	39	37	43
Fleet cards	22	15	29	32	32
"One card" combining several uses above	19	23	16	15	11
Airline travel cards (UATP)	7	5	8	6	11

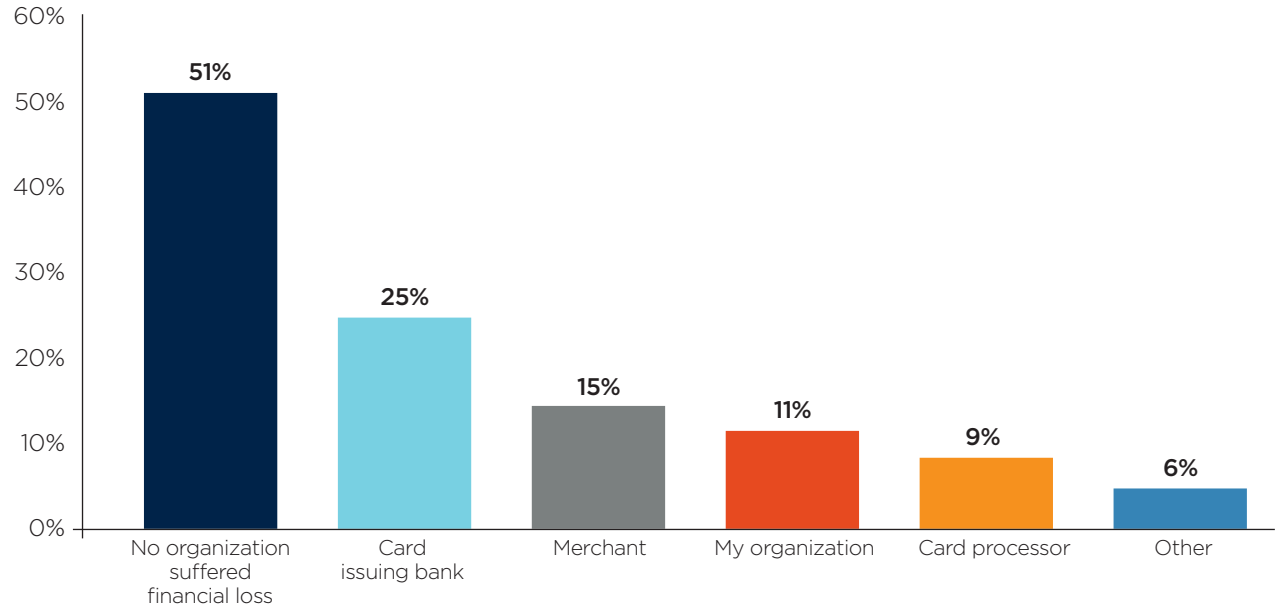
©2017 Association for Financial Professionals, Inc. All Rights Reserved

Twenty-seven percent of organizations that experienced payments fraud in 2016 were impacted by fraud associated with their own corporate commercial cards, a significant decline from the 42 percent reported for 2015. Corporate/commercial cards were the third most targeted payment method by fraudsters in 2016.

Corporate/commercial card fraud can result in financial loss not only to organizations but also to third parties such as an organization's bank or merchant partners. In 2016, over half of organizations did not suffer a financial loss from corporate/commercial card fraud—an increase from the 38 percent in 2015. A smaller share of organizations' merchants also experienced an increase in corporate/commercial card fraud—from 21 percent in 2015 to 15 percent in 2016. Eleven percent of finance professionals report their organizations suffered financial loss from such fraud.

Cards are the payment method that has experienced the most volatile trend in fraud. As mentioned above, the incidence of fraud via corporate/commercial card appears to correlate with data breaches in which large numbers of card credentials are stolen. In the aftermath of such data breaches, card fraud seems to increase. However, there can also be a time lag between when card credentials are stolen and when fraudulent cards/credentials are actually used. One reason for the recent decline in card fraud—from 39 percent in 2015 to 32 percent in 2016—may be that card issuers and banks have become more proficient in protecting the data. Another reason may be quicker action of canceling cards when data breaches occur.

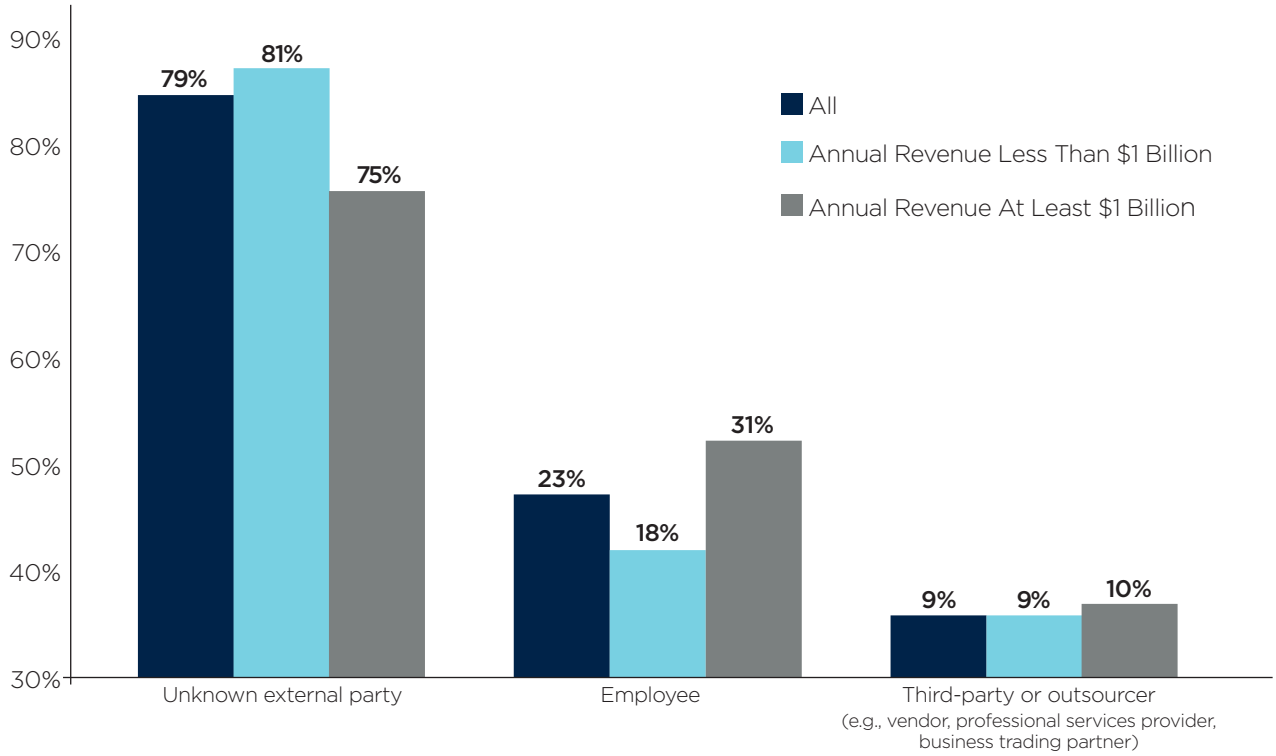
Parties That Suffered Financial Loss from Fraud on Corporate/Commercial Cards
(Percent of Organizations that Suffered At Least One Attempt of Corporate/Commercial Card Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

For a large majority of companies (79 percent) that experienced fraud via their own corporate/commercial cards in 2016, the fraud was perpetrated by an unknown external party. This result is similar to the 77 percent reported for 2015. For 23 percent of these organizations, this type of fraud was initiated by an employee, an increase from 17 percent in 2015—an increase especially troubling since the fraud is committed by individuals who have been trusted by the organization that was the target of the fraud. Larger organizations with annual revenue of at least $1 billion were more likely than smaller companies to be impacted by fraud committed by an employee (31 percent versus 18 percent). Indeed, larger organizations experienced the most significant increase in card fraud committed by employees—from 23 percent in 2015 to 31 percent in 2016. Corporate/commercial card fraud committed by a third-party or outsourcer (e.g., vendor, professional services provider) decreased from 14 percent in 2015 to nine percent in 2016.

Party Responsible for Fraud on Corporate/Commercial Cards
(Percent of Organizations that Experienced At Least One Attempt of Corporate/Commercial Card Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Half of the survey respondents whose companies were exposed to corporate/credit card fraud report that the financial loss experienced by their organizations as a consequence of the fraud was due to fraudulent credit card charges made by a third party. Other plausible causes for loss are employee theft (39 percent) and lack of internal controls (25 percent). A greater share of finance professionals from large organizations with more than 100 payment accounts than those from similar-sized companies with fewer payment accounts indicate that fraudulent credit card charges by a third-party company is a reason for the financial loss those companies experienced (67 percent versus 50 percent).

Reasons for Financial Loss Associated with Corporate/Commercial Cards
(Percent of Organizations that Experienced At Least One Attempt of Corporate/Commercial Card Fraud)

	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
Fraudulent credit card charges made by a third party	50%	44%	52%	50%	67%
Employee theft	39	44	39	50	17
Lack of internal controls	25	33	17	17	17
No segregation of duties	5	6	4	–	–

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Mobile Payments

Mobile devices have been available for B2B transactions for a number of years. It is, however, important to define what mobility means for corporate transactions. Rather than using mobile wallets to conduct payments, mobility for corporations is more about using online banking functionality and authorization of payments, etc., from a mobile device. If key personnel are out of the office, mobile devices can be very effective in ensuring minimal interruption to payment schedules and processes.

Security of **mobile payments** continues to be of concern to survey respondents

The overriding concern about mobile payments continues to be security (cited by 72 percent of respondents). Security of mobile payments is of greater concern to larger organizations with more than 100 payment accounts than to those with fewer accounts (87 percent versus 68 percent).

Fifty-five percent of corporate practitioners report their companies are also hesitant to adopt mobile payments because of concerns about potential exposure of personal financial information resulting from the loss of a smartphone. Concern about transmission of financial data over cell phone networks is preventing nearly half of companies (49 percent) from adopting mobile payments more extensively. A greater share of finance professionals from larger organizations with annual revenue of at least $100 billion are more apprehensive about transmitting data over cell phone networks and the authentication process than are their peers from smaller companies.

Security Issues Preventing Consumers from Further Embracing Mobile Payments
(Percent 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
Concerns about whether mobile payments are a secure payment method	72%	75%	73%	68%	87%
Potential exposure of personal financial information resulting from a loss of smartphone	53	56	54	55	50
Transmitting financial data over cell phone networks	49	46	54	53	47
The authentication process	29	27	33	37	30

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Credit/Debit Card Payments

Seventy percent of corporate practitioners report that their companies accept debit/credit card payments from their vendors and customers. A greater share of larger organizations accepts debit/credit card payments than do smaller organizations (75 percent versus 68 percent).

Adoption of EMV technology, which authenticates chip card transactions, has been slow in the U.S. The EMV liability shift in October 2015 was not a mandate that required businesses to accept EMV cards, but rather a shift of liability from the card issuers to merchants without the capability to accept the new EMV-enabled cards. Businesses could opt out of investing in new terminals, as has been the cases for many businesses in high-volume, low-value businesses, such as fast-food restaurants. The low level of fraud among these businesses simply did not justify investing in new EMV-enabled terminals.

Also, adoption of EMV has not been painless. There has been a shortage of terminals capable of accommodating the new technology and this has caused delays. Certification of these terminals has also seen delays. The result has been slow implementation.

As the use of EMV chip cards becomes more prevalent, fraudsters are likely to shift their focus to less secure payment methods. Ninety-three percent of survey respondents believe this will be the case if perpetrators are less successful in hacking credit/debit cards. This is slightly higher than the 90 percent of finance professionals who held this view in 2015 but 23 percentage points higher than in 2014. Sixty-two percent of finance professionals anticipate that the instances of fraud will increase for those transactions where cards are not present, e.g., online transactions. This is an increase from 55 percent reported for 2015. A smaller share of finance professionals anticipate fraud activity in checks and wire transfers will increase as a result of EMV cards being used more extensively (15 percent and eight percent, respectively).

Forms of Payments Subject to Greater Fraud Activity if EMV Cards are Successful in Reducing Fraud
(Percentage Distribution of Respondents)

	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
Card-not-present transactions	62%	62%	65%	56%	60%
Checks	15	16	13	9	16
Wire transfers	8	8	9	9	12
ACH debit	5	5	5	7	4
ACH credit	1	1	2	2	–
Fraud won't migrate to other payment forms	7	9	6	4	8

©2017 Association for Financial Professionals, Inc. All Rights Reserved

A vast majority (91 percent) of finance professionals believes that EMV chip cards will be successful in mitigating point-of-sale (POS) fraud. Sixty-nine percent consider Chip-and-PIN an effective method in reducing POS fraud, as a four-digit PIN would add an additional layer of security for cards. Other methods considered effective are Chip-and-Choice, in which a merchant can choose the option of signature or PIN (cited by 10 percent of respondents), and chip and signature (four percent). Finance professionals from larger organizations with more than 100 payment accounts are less likely than those with fewer payment accounts to consider Chip-and-PIN to be effective in preventing POS fraud.

The EMV technology does help prevent counterfeiting of cards. But it comes as no surprise that as the EMV card technology is being implemented, fraud has migrated elsewhere, especially to card-not-present (CNP) transactions.

91% of finance professionals believe that **EMV chip cards** will be successful in mitigating point-of-sale (POS) fraud

Authentication Method for EMV Cards Most Effective in Preventing Fraud and Providing a Better Customer Experience
(Percentage Distribution of Respondents)

	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
Chip-and-PIN	69%	68%	70%	76%	52%
Chip-and-Choice (merchant can chose PIN or Signature)	10	11	7	2	20
EMV is effective in reducing POS card fraud regardless of authentication method used	9	8	10	9	8
Don't believe EMV is effective in reducing POS card fraud (i.e., no authentication method will be effective in reducing POS card fraud)	9	9	9	9	12
Chip-and-Signature	4	4	4	3	8

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Securing Credentials

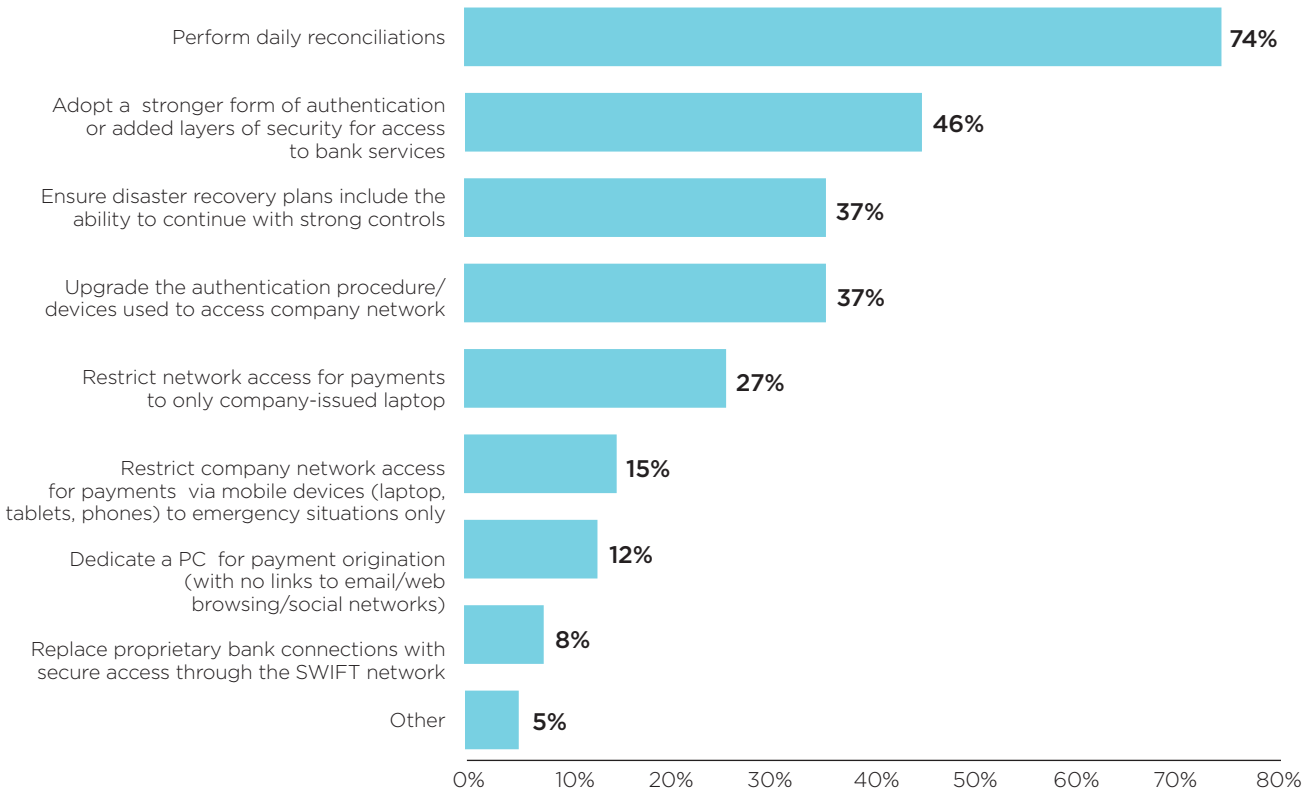
Cyberattacks, data phishing and data breaches have become an almost daily occurrence. Malicious emails with virus-infested links are rampant. Even though these emails are often easy to detect, the sheer volume of such emails suggests that if a fraction of them are opened they could provide a door for criminals to gather valuable information and potentially compromise vital systems.

Organizations are well aware that a fraud attack and data breach can have far-reaching consequences for both their bottom line and reputation. They are taking serious steps to alleviate any fraud attacks and minimize the impact if they are targeted. Nearly three-fourths ***are performing daily reconciliations*** to protect themselves against attacks that would compromise security. Other strategies being implemented by organizations are:

- Adopt a stronger form of authentication or added layers of security for access to bank services (cited by 46 percent of survey respondents)
- Upgrade the authentication procedure/devices to access their company network (37 percent)
- Ensure disaster recovery plans include the ability to continue with strong controls (37 percent)
- Restricting network access for payments to only company-issued laptops (27 percent)

As mentioned earlier, it is important to realize that it is almost impossible to protect against all fraud. Given sufficient time and resources, criminals can hack into almost any system. What organizations *can* do is to make it more difficult for criminals to gain access. If criminals are met with resistance they will most likely move on to an easier target. Using several layers of security is generally a good way to safeguard an organization's internal systems. Particular effort should be placed on payment systems. One way is restricting network access for payments to specific company-issued computers that only are used for payment transactions.

Actions Taken to Defend Against Attacks that Would Compromise Security
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



©2017 Association for Financial Professionals, Inc. All Rights Reserved

Conclusion

Results from the *2017 AFP Payments Fraud and Control Survey* suggest that the spike in payments fraud observed in 2015 was not an anomaly. In 2016, AFP reported 73 percent of organizations in 2015 had been exposed to attempted/actual payments fraud—a significant 11-percentage-point increase from 2014. This year's survey results are very comparable, as 74 percent of survey participants indicate their organizations were exposed to either attempted or actual fraud in 2016.

Although the high incidence of fraud does not necessarily translate into significant impacts on companies' bottom lines, it can negatively impact an organization's reputation and expose confidential business and personnel information, putting companies, their employees and their customers at significant risk.

Business leaders are aware that fraudsters are actively looking to infiltrate organizations' payment systems, and consequently they are making serious efforts to safeguard against such attacks in order to prevent and minimize any possible damage any breaches may cause. Our research shows business leaders are cognizant of what might be making their companies more vulnerable, and those leaders are seeking ways to institute effective controls. Unfortunately, perpetrators of payments fraud are usually a step ahead and are increasingly successful in circumventing any checks and controls organizations have in place.

Fraudsters are relentless. Even if they do face challenges when attempting to hack into payment systems, they are becoming more resourceful and shifting their focus to more vulnerable methods. Business email compromise (BEC) is an example of a "newer" type of fraud being conducted more extensively. Unsuspecting employees receive emails from fraudsters who pose as an organization's senior executives, requesting staff to wire funds and share personal and confidential information. Many have fallen for the hoax and exposed themselves and their companies to fraud. Our survey results indicate a continued uptick in BEC with nearly three quarters of survey participants reporting their organizations had experienced fraud via this avenue in 2016.

Executive teams at organizations will need to increasingly focus on protecting their businesses from fraud. Often these attacks originate in other countries, making it even more challenging to capture those committing fraud. Safeguarding payment systems, investing in secure controls, and constantly striving to stay "one step ahead" of fraudsters will be even more essential for businesses going forward.

Key highlights revealed in the *2017 AFP Payments Fraud and Control Survey*:

- **Seventy-four percent** of finance professionals report that their companies **were victims of payments fraud in 2016**. This is the highest percentage on record.
- **Checks** continue to be the payment method most frequently targeted by those committing or attempting to commit fraud. **Seventy-five percent** of organizations that were victims of fraud attempts/attacks in 2016 experienced check fraud.
- **Almost two-thirds of companies (63 percent)** that experienced attempted or actual payments fraud in 2016 did so as a result of **actions by an outside individual**.
- **Seventy-four percent** of finance professionals report that their organizations **were victims of business email compromise (BEC)** in 2016. This is a 10-percentage-point increase from 2015.
- **Over 70 percent** of corporate practitioners report that their organizations are being proactive and **have implemented controls to prevent any impact from BEC**.
- **Seventy-two percent** of respondents have concerns about the **extent of security** of mobile payments.

©2017 Association for Financial Professionals, Inc. All Rights Reserved

About the Survey

In January 2017, the Research Department of the Association for Financial Professionals® (AFP) surveyed corporate practitioner members and prospects with the following job titles: cash manager, analyst and director. The survey yielded 311 responses from members and an additional 236 responses from prospects for a total of 547 responses.

AFP thanks J.P. Morgan for underwriting the *2017 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.

Industry Classification

(Percentage Distribution of Organizations)

Banking/Financial services	5%
Business services/Consulting	6
Construction	2
Energy (including utilities)	9
Government	7
Health services	9
Hospitality/Travel	2
Insurance	6
Manufacturing	20
Non-profit (including education)	8
Real estate	6
Retail (including wholesale/distribution)	9
Software/Technology	5
Telecommunications/Media	2
Transportation	3

Types of Organization's Payment Transactions

(Percentage Distribution of Organization's Payment Transactions)

	When Making Payments	When Receiving Payments
Primarily businesses	72%	49%
Split between consumers and businesses	25	30
Primarily consumers	3	21

Number of Payment Accounts Maintained

(Percentage Distribution of Organizations that Experienced Payments Fraud)

	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	27%	37%	19%	33%	—
5-9	18	25	13	23	—
10-25	20	15	25	44	—
26-50	11	7	14	—	—
51-100	9	7	13	—	—
More than 100	15	10	15	—	100%

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Annual Revenues (USD)

(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
Under $50 million	8%	16%	—	—	—
$50-99.9 million	3	5	—	—	—
$100-249.9 million	10	21	—	—	—
$250-499.9 million	9	18	—	—	—
$500-999.9 million	20	40	—	—	—
$1-4.9 billion	30	—	58%	69%	29%
$5-9.9 billion	10	—	19	17	13
$10-20 billion	7	—	13	9	26
Over $20 billion	6	—	11	6	32

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
Privately held	41%	53%	28%	30%	19%
Publicly owned	36	21	51	43	74
Non-profit (not-for-profit)	13	14	11	15	3
Government (or government-owned entity)	11	12	10	13	3

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Appendix

Payment Method Subject to Attempted and/or Actual Payments Fraud in 2016

(Percent 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	All (2015)
Checks					
55%	44%	66%	65%	65%	52%
Wire transfers					
34	35	40	35	48	27
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)					
23	27	24	24	29	29
ACH debits					
22	20	25	20	35	18
ACH credits					
8	4	10	8	16	8
Organization was not a victim					
26	29	19	18	16	27

Payment Method Subject to Attempted and/or Actual Payments Fraud in 2016

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

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion
Checks	75%	61%	81%
Wire transfers	46	49	49
Corporate/commercial credit cards (e.g., purchasing, T&E, fleet)	32	38	29
ACH debits	30	52	31
ACH credits	11	20	12

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Change in Incidence of Payments Fraud in 2016 Compared to 2015

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

	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
More	36%	35%	42%	43%	42%
About the same	55	57	49	49	42
Less	9	9	9	9	15

Sources of Attempted/Actual Payments Fraud in 2016

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

	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
Outside individual (e.g., check forged, stolen card)	63%	60%	66%	69%	58%
Business Email Compromise	52	55	51	51	42
Organized crime ring	14	12	18	19	15
Third-party or outsourcer	13	8	18	13	27
Account takeover (e.g., hacked system, malicious code—spyware or malware from social network)	13	13	13	12	15
Internal party	5	1	8	7	15
Compromised mobile device	2	1	1	–	4
Lost or stolen laptop	1	1	1	–	4
Other	6	7	5	3	4

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Percent of Organizations that Experienced Attempted and/or Actual Business Email Compromise (BEC) Fraud in 2016

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

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes	74%	76%	77%	73%	88%
No	26	24	23	27	12

Payment Methods Impacted by Actual Loss as a Result of Business Email Compromise

(Percent of Organizations that Experienced a Financial Loss Due to Business Email Compromise)

	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
Wire transfers	60%	61%	64%	59%	60%
Checks	32	22	33	35	30
ACH Credits	16	11	14	12	20
Corporate/Commercial credit and debit cards	16	22	14	12	20
ACH Debits	6	6	8	6	20

Change in incidence of Check Fraud in 2016 Compared to 2015

(Percentage Distribution of Organizations Subject to Attempted and/or Actual Payments Fraud via Checks)

	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
Increased	20%	19%	23%	19%	27%
About the same	68	67	67	74	63
Decreased	12	14	11	7	10

Organization Suffered Financial Loss as a Result of Check Fraud

(Percentage Distribution of Organizations that Experienced At Least One Attempt of Check Fraud)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes	10%	8%	12%	12%	6%
No	90	92	88	88	94

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Reasons for Financial Loss Due to Check Fraud

(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)

	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
No positive pay	23%	31%	13%	14%	–
Clerical errors	18	8	26	21	100%
Internal fraud (e.g., employee responsible)	15	15	13	7	–
Account reconciliation not timely	15	23	9	7	–
Stolen check stock	15	23	13	14	–
Gaps in online security controls/criminal account takeover	13	8	17	14	50
Other	33	23	39	43	–

Change in Incidence of ACH Fraud in 2016 Compared to 2015

(Percentage Distribution of Organizations that Experienced At Least One Attempt of ACH Fraud)

	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
Increase	13%	7%	21%	20%	14%
About the same	80	85	72	73	79
Decreased	7	7	7	7	7

Suffered Financial Loss as a Result of ACH Fraud

(Percentage Distribution of Organizations that Experienced At Least One Attempt of ACH Fraud)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes	5%	2%	9%	7%	16%
No	95	98	91	93	84

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Reasons for Financial Loss from ACH Fraud

(Percent of Organizations that Experienced At Least One Attempt of ACH Fraud)

	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
ACH return not timely	33%	25%	31%	29%	20%
Gaps in online security controls/criminal account takeover	29	–	38	29	80
Did not use ACH debit blocks or ACH debit filters	24	75	13	14	–
Did not use ACH positive pay	14	25	13	29	–
Internal fraud (e.g., employee responsible)	14	–	19	14	20
Account reconciliation not timely	10	25	6	–	–

Fraud Control Procedures Used to Prevent ACH Fraud

(Percent of Organizations that Experienced At Least One Attempt of ACH Fraud)

	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
Reconcile accounts daily to identify and return unauthorized ACH debits	60%	75%	53%	57%	25%
Block all ACH debits except on a single account set up with ACH debit filter/ACH positive pay	50	25	60	71	50
Create separate account for electronic debits initiated by the third party (e.g., taxing authority)	35	25	40	43	50
Block ACH debits on all accounts	30	25	33	29	50
Debit block on all consumer items with debit filter on commercial ACH debits	10	25	7	–	25

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Organization's Own Corporate/Commercial Cards Used in Attempt to Commit Fraud

(Percentage Distribution of Organizations that Experienced At Least One Attempt of Corporate/Commercial Card Fraud)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes	27%	30%	25%	22%	32%
No	73	70	75	78	68

Party Responsible for Fraud on Corporate/Commercial Cards

(Percent of Organizations that Experienced At Least One Attempt of Corporate/Commercial Card Fraud)

	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
Unknown external party	79%	81%	75%	63%	90%
Employee	23	18	31	38	30
Third-party or outsourcer	9	9	10	8	30

Parties that Suffered Financial Loss from Fraud on Corporate/Commercial Cards

(Percent of Organizations that Experienced At Least One Attempt of Corporate/Commercial Card Fraud)

	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
No organization suffered financial loss	51%	54%	8%	8%	14%
Card-issuing bank	25	23	13	11	21
Merchant	15	18	27	27	28
My organization	11	10	49	49	41
Card processor	9	10	11	11	10

©2017 Association for Financial Professionals, Inc. All Rights Reserved

Acceptance of Credit and/or Debit Card Payments from Customers
(Percentage Distribution of Organizations)

	All	Annual Revenue Less Than $1 Billion	Annual Revenue At Least $1 Billion	Annual Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Annual Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes	70%	68%	75%	77%	84%
No	30	32	25	23	16

Actions Taken to Defend Against Attacks that Would Compromise Security
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)

	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
Perform daily reconciliations	74%	71%	76%	84%	50%
Adopt a stronger form of authentication or added layers of security for access to bank services	46	43	48	42	50
Upgrade the authentication procedure/devices used to access company network	37	34	38	36	54
Ensure disaster recovery plans include the ability to continue with strong controls	37	33	41	41	38
Restrict company network access for payments to only company-issued laptop	27	25	27	26	23
Restrict network access for payments via mobile devices (laptop, tablets, phones) to emergency situations only	15	16	14	12	8
Dedicate a PC for payment origination (with no links to email/web browsing/social networks)	12	9	12	12	4
Replace proprietary bank connections with secure access through the SWIFT network	8	5	10	6	23

©2017 Association for Financial Professionals, Inc. All Rights Reserved

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 the Association for Financial Professionals

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional™ and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators™ serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.

AFP, Association for Financial Professionals, Certified Treasury Professional, and Certified Corporate Financial Planning & Analysis Professional are registered trademarks of the Association for Financial Professionals. © 2017 Association for Financial Professionals, Inc. All Rights Reserved.

General Inquiries	AFP@AFPonline.org
Web Site	www.AFPonline.org
Phone	301.907.2862

Commercial Banking Treasury Services

J.P.Morgan

© 2017 JPMorgan Chase Bank, N.A. Member FDIC. "Chase" is a marketing name for certain businesses of JPMorgan Chase & Co. and its subsidiaries (collectively, "JPMC"). 304323