ASSOCIATION FOR FINANCIAL PROFESSIONALS

2019 AFP®

PAYMENTS FRAUD AND CONTROL SURVEY REPORT

Comprehensive Report

Underwritten by J.P.Morgan

Table Of Contents

J.P.Morgan has been the proud sponsor of the AFP Payments Fraud and Control Survey for 11 consecutive years, and we are pleased to deliver the 2019 report.

The survey showed that 82 percent of companies were targets of payments fraud last year, demonstrating the crucial need for cybersecurity protocols and strict control governance. Additionally, the survey revealed that in 2018:

- 80 percent of organizations experienced Business Email Compromise (BEC)
  - 54 percent of organizations reported financial losses as a result of BEC
  - 70 percent of BEC scams targeted checks, followed by wires at 43 percent
- 70 percent of organizations experienced check fraud, a slight decrease from 2017
- 64 percent of attempted or actual payments fraud resulted from actions of an individual outside the organization
- One-fourth of organizations indicated they have not received any advice from their banks, regarding mitigating potential additional risks with same-day ACH operational for both credit and debit transactions.

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 safeguard corporate assets and data from cyber fraud. It is equally important for all businesses to consider and mitigate against non-financial implications of payments fraud. Should a fraud attack expose personal or confidential information, businesses stand to suffer reputational risk, which can be severe, expensive and require significant clean-up efforts.

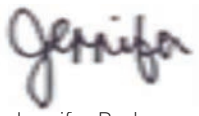
J.P. Morgan is one of the world's largest providers of treasury management services and is a leader in electronic payments technology and solutions. We are committed to fraud mitigation and information protection across our entire infrastructure, and we will continue to invest in the technology, educational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

We hope this survey serves as an important tool in understanding the potential cyber risks within your organization, which 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 against payments fraud is to remain vigilant in detection and cybersecurity protection protocols.

With best regards,

Jessica Lupovici
Managing Director
J.P. Morgan

Bob St Jean
Managing Director
J.P. Morgan



Jennifer Barker
Managing Director
J.P. Morgan

Chad Prescott
Managing Director
J.P. Morgan

Winston Fant
Managing Director
J.P. Morgan

Introduction

Payments fraud activity appears to be the "new normal" at organizations today. Indeed, there are few signs that payments fraud activity is declining; payments fraud activity has been increasing steadily since 2013 and in 2018 reached a new peak. **More than 80 percent of financial professionals report that their organizations were targeted by fraudsters in 2018, the largest percentage since the Association of Financial Professionals® (AFP) began tracking such activity.** Organizations are cognizant of increasing threats and in many cases are actively implementing measures to control payments fraud. But that increased vigilance is not always enough; the tactics of those engaging in payments fraud are more sophisticated and, consequently, more fraudsters are successful in infiltrating targeted organizations.

Checks are the most frequently used payment method for business-to-business transactions and are, therefore, common targets of fraudsters. While checks continue to be the payment method most often affected by fraud activity, check fraud is declining. **Check fraud has declined since 2010, and in 2018 was at its lowest level since AFP began its payments fraud survey series.** While technology advancements are making processes surrounding electronic payments easier, those same technologies are also helping perpetrators in their attempts to attack payment methods. **The decline in check fraud activity has been offset by the increase in payments fraud via wire transfers and ACH debits and credits**.

Business Email Compromise (BEC) is a relatively new type of fraud activity that has been increasing since it was first recognized. **The percentage of organizations falling prey to BEC scams has increased from 64 percent in 2014 to 80 percent in 2018.** This is troubling since fraud via BEC is no longer a new phenomenon. Most organizations are aware of this type of fraud and many have implemented additional controls to protect themselves from being victims. BEC fraudsters are innovative and devise ways that can "morph" their fraud attempts into new and unexpected forms, thus continuing to scam their targets.

AFP has noted that, historically, financial losses incurred as a result of payments fraud activity are not extensive. This, however, does not suggest that payments fraud can or should be taken lightly. Nonfinancial impacts of successful payments fraud activity can be crippling. In addition to adversely affecting an organization's reputation, payments fraud can expose confidential information and require significant clean-up efforts. Investing upfront in training and controls is essential in obstructing fraud activity that can result in significant outlays of money and time.

Financial professionals need to be proactive if they want to prevent and mitigate the effects of payments fraud successfully. Besides minimizing the known threats being targeted at their companies, they have to predict the unknowns and prevent such threats from having an impact. This is challenging and requires significant investments of time and money as well as an organization leadership committed to minimizing these crimes.

Every year since 2005, the Association for Financial Professionals® has conducted its *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 from fraudsters. Continuing this research, AFP conducted the 15th Annual *Payments Fraud and Control Survey* in January 2019. The survey generated 617 responses from corporate practitioners from organizations of varying sizes representing a broad range of industries. Results presented in this report reflect data for 2018. 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. AFP's Research department is solely responsible for both the questionnaire design and the final report, along with its content and conclusions.

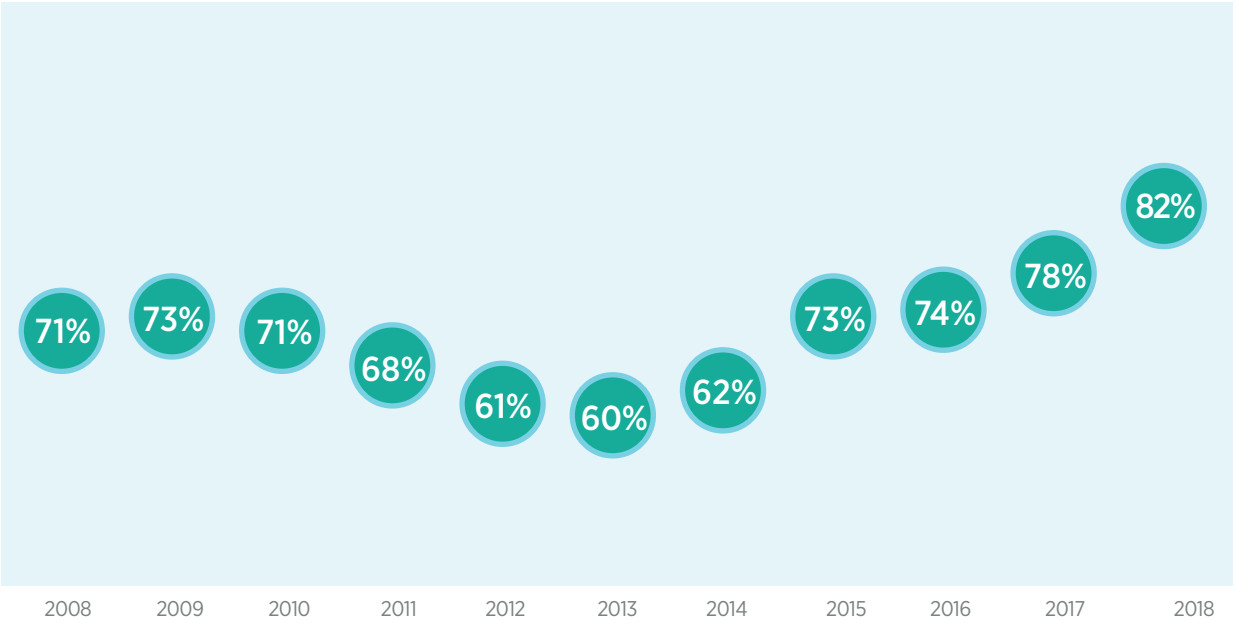
01 PAYMENTS FRAUD ACTIVITY

Another Surge in Payments Fraud Activity

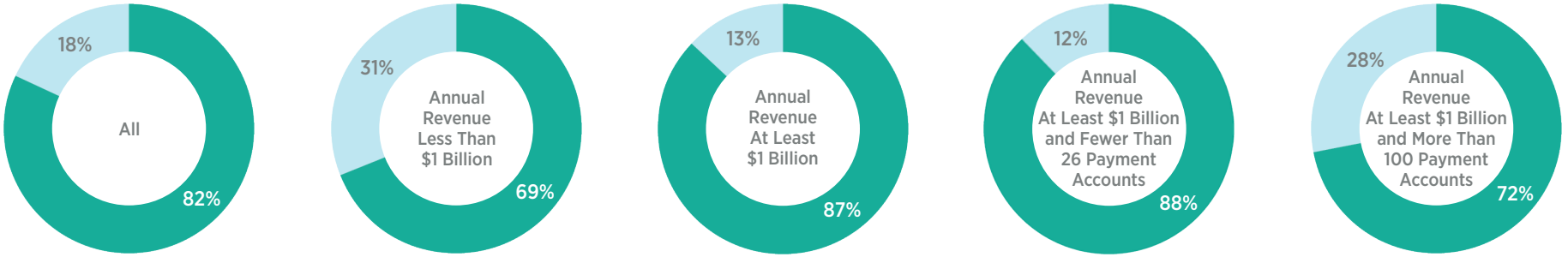
In the past five years payments fraud activity has increased dramatically. **A record-setting 82 percent of financial professionals report that their organizations experienced attempted and/or actual payments fraud in 2018**, four percentage points higher than the previous record in 2017 and 20 percentage points higher than the share in 2014.

Larger organizations (with annual revenue of at least $1 billion) are more susceptible to payments fraud attacks than are smaller ones (with annual revenue less than $1 billion): 87 percent compared to 69 percent, respectively. The difference between the share of larger organizations and smaller ones that are victims of fraud has also been widening—from a seven-percentage-point difference in 2017 to 18 percent currently. Also, for a fourth consecutive year, larger organizations with fewer than 26 payment accounts appear to be easier targets than organizations of the same size with more than 100 payment accounts.

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2008-2018



Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2018



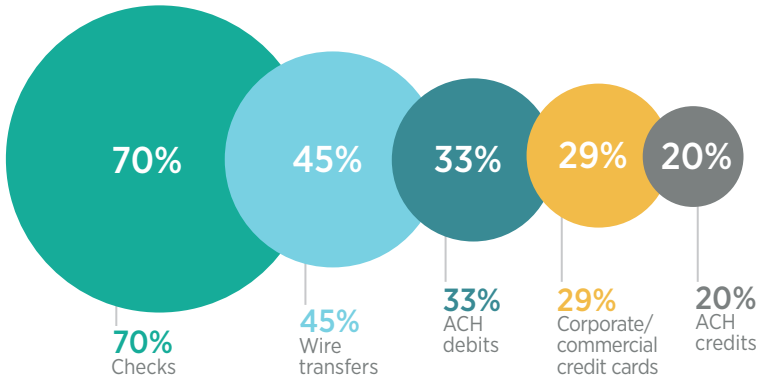
Decreased Fraud Activity in Checks and Wire Transfers, but a Noticeable Increase in Fraud Activity in ACH Credits and Debits

Although checks and wire transfers continued to be the payment methods most impacted by fraud activity in 2018 (70 percent and 45 percent, respectively), the percentage of financial professionals reporting fraud activity via these two payment methods has decreased in the past year. Seventy-four percent of financial professionals reported their organizations' check payments were subject to fraud attempts/attacks in 2017 while 70 percent report the same for 2018. In fact, payments fraud via checks has been on the decline since 2010. The share of organizations that were victims of fraud attacks via wire transfers also decreased slightly, from 48 percent in 2017 to 45 percent last year. The decline in wire fraud, however, is slight and may not indicate a downward trend. Wire fraud activity continues to be high, especially considering the share of organizations experiencing such fraud was only in the single digits until 2012. There has since been an increase in the percentage of organizations reporting wire fraud.

This year's survey results reveal a noticeable increase in fraud activity via both ACH credits and ACH debits. Thirty-three percent of financial professionals report their organizations' payments via ACH debits were subject to fraud attempts/attacks in 2018; that is an increase of five percentage points from 2017. Fraud activity via ACH credits increased seven percentage points from 2017 to 20 percent in 2018.

This new development indicates that fraudsters are now trying to use ACH transactions as vehicles for their scams as they move away from checks and wires. As ACH transactions are typically considered safer and more difficult to compromise, the increase in ACH fraud suggests that such fraud is of a more sophisticated kind. In their attempts to alter the way they conduct their scams and to avoid raising any red flags, fraudsters may think that shifting to an unexpected payment method can do just that—help them avoid detection. In these cases it is usually not the payment method itself that is compromised but *the processes leading up to payment initiation*. It is also possible that in order to conduct scams via ACH transactions, fraudsters may either compromise internal systems through phishing attacks or recruit assistance from inside their target organizations to help facilitate ACH transaction initiation.

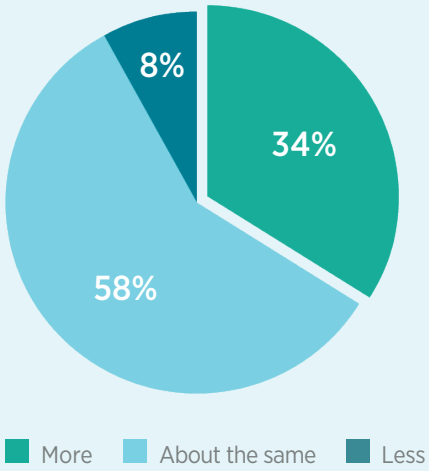
Payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2018
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



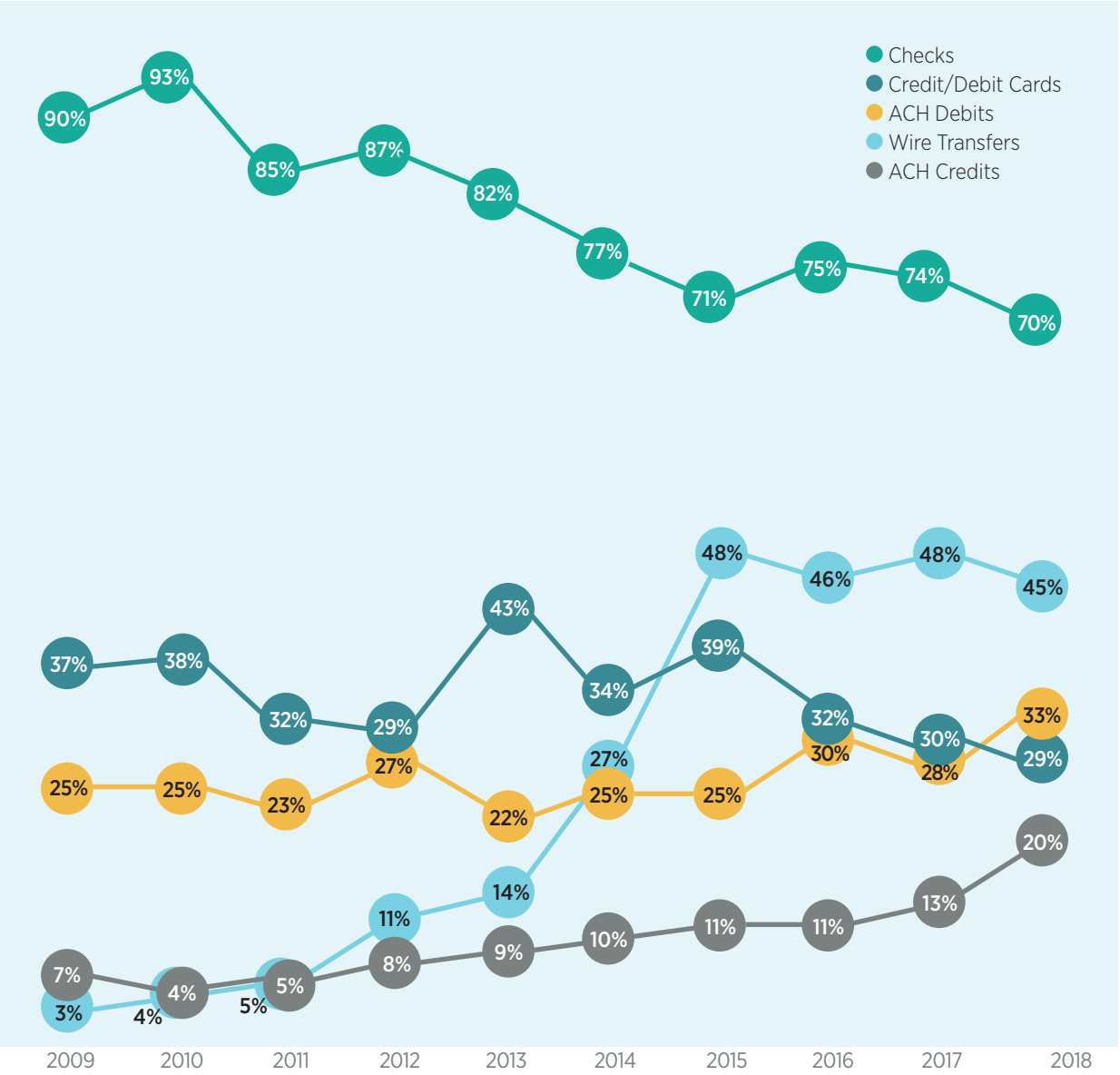
For a Majority of Companies, Payments Fraud Is Unchanged while Slightly More than One-third See an Increase

While 58 percent of financial professionals report no change in the incidence of payments fraud in 2018 compared to 2017, 34 percent note there has been an increase. Eight percent report a decline.

Change in Incidence of Payments Fraud in 2018
(Percentage Distribution of Organizations that Experienced Attempted and/or Actual Payments Fraud)



Historical data, 2009-2018



Historical Trend of Fraud for Payment Methods

- Checks are the payment method most subject to fraud, but instances being reported are on the decline
- Wire fraud continues to be at elevated levels, Business email Compromise (BEC) a likely cause of attacks
- Fraud activity with cards on the decline
- ACH debit fraud has increased to record levels and continues its upward trend
- A steady increase in ACH credit fraud since 2012

Checks Continue to be Popular Targets for Fraudsters

Checks have been and continue to be the payment method most often exposed to fraudulent activity. Thirty-eight percent of organizations that experienced check fraud in 2018 suffered between one and five incidents of such fraud and 25 percent were subject to between six and ten incidents. Larger organizations with more than 100 payment accounts were far more likely to have suffered a greater number of instances of check fraud than were other companies; 29 percent of survey respondents from this group report that their organizations experienced check fraud more than 15 times in 2018.

These results suggest that it is challenging for finance/treasury staff to monitor a large number of accounts for payments fraud, and so when fraud attempts are made, they may not be discovered right away. Having fewer accounts would naturally mean they are easier to oversee; thus, it would be easier to detect any fraud attempts. When fraudsters do succeed in their scams, their success encourages more attacks on the same targets since scammers are aware of those targets' vulnerability. Companies that have been victims are prone to be targeted frequently. We see this trend in both checks and ACH.

Number of Times Organization Experienced Attempted and/or Check Fraud in 2018
(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
1-5	38%	52%	34%	37%	30%
6-10	25%	26%	25%	22%	24%
11-15	12%	6%	14%	15%	16%
16-20	4%	2%	5%	5%	5%
More than 20	20%	14%	22%	20%	24%

Paper checks are still used extensively in the U.S. for business-to-business (B2B) transactions and they account for a significant share of payments. The *2016 AFP Electronic Payments Report* revealed that 51 percent of B2B payments are made by check. This is likely one reason checks are the most popular targets for payments fraud. It is important to note, however, that even though checks are frequent targets of fraudsters, there has been a decline in check fraud activity since 2010. Even as the use of checks declines, it is unlikely that the overall level of fraud activity will abate since fraudsters will likely shift attention to other payment methods and tactics. This is evident in the increasing incidence of payments fraud via Business Email Compromise and wire transfers.

Corporate/Commercial Credit/Debit Cards Prone to Payments Fraud Attacks

Twenty-nine percent of treasury and finance professionals report their organizations were subject to corporate/commercial credit/debit card fraud in 2018. Such fraud has declined steadily since 2015.

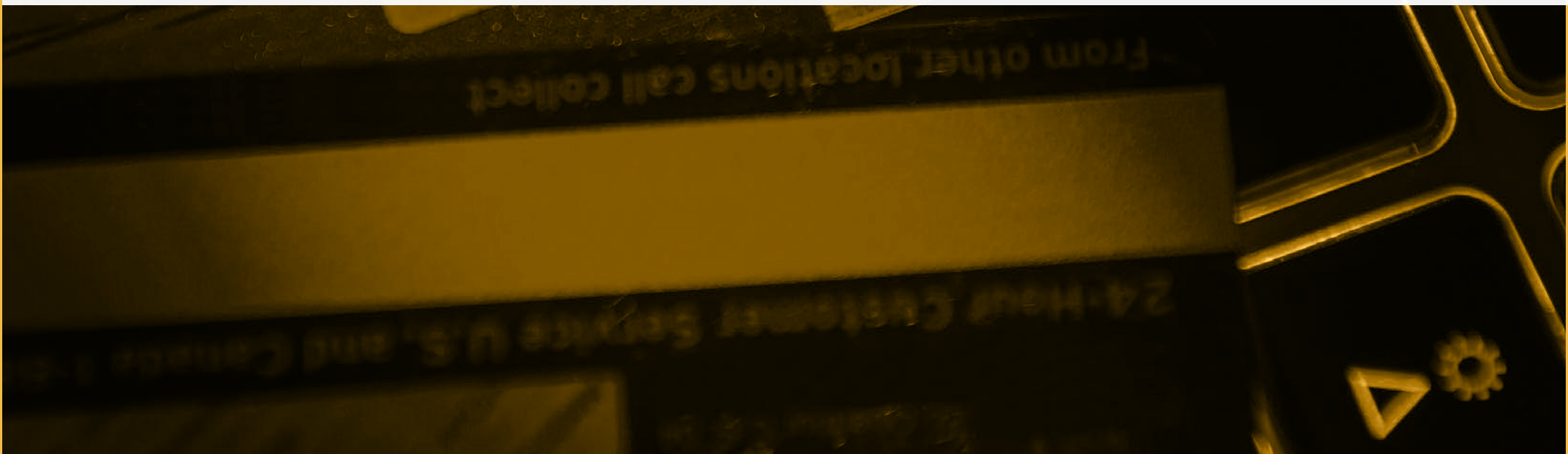
A few years ago, a number of high-profile retailers were exposed to significant card fraud activity. That experience encouraged them to move from paper-based payment methods to electronic payments. The use of corporate/commercial cards declined as a result and has not rebounded. The decreased use of cards is one possible reason card fraud has declined. Another development that likely has contributed to this trend is the "liability shift" resulting from the transition from magnetic stripe cards to smart-chip cards which are much more difficult to counterfeit. Finally, banks' use of technology such as "algorithms" and "machine learning for spend patterns" has also contributed to card fraud being detected at an early stage and so easier to contain.

The corporate/commercial cards most prone to fraud in 2018 were Travel & Entertainment Cards (T&E Cards), used by 57 percent of organizations followed by purchasing cards (54 percent). Twenty-three percent of practitioners report their companies suffered a loss as a result of corporate/commercial card fraud. The primary causes of corporate/commercial card fraud are fraudulent credit card charges made by a third party vendor (18 percent), followed by employee theft/initiated by an employee (10 percent).

Percent of Organizations that Experienced Payments Fraud through Corporate/Commercial Credit/Debit Cards, 2009-2018

02

PAYMENTS FRAUD: COSTS INCURRED, SOURCES AND TIME TO DISCOVER



How Does Payments Fraud Impact the Bottom Line?

Financial Loss from Fraud Attempts

Financial leaders at organizations are cognizant of the impact payments fraud attempts/activity can have on their organizations. They are well aware that fraud can result not only in financial losses, but could also expose confidential company information and adversely affect an organization's reputation. Potential losses from attacks range from $0 to more than $2 million. Forty-five percent of organizations face potential financial losses totaling less than $100,000 as a result of fraud activity in 2018. Ten percent of financial professionals report there are no potential losses at their companies, while a full 12 percent indicate that $2 million or more may be lost.

Potential Financial Loss from Attempted and/or Actual Payments Fraud in 2018

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

TOTAL DOLLAR AMOUNT	
Zero	10%
Up to $24,999	24%
$25,000-49,999	10%
$50,000-99,999	11%
$100,000-249,999	15%
$250,000-499,999	9%
$500,000-999,999	5%
$1,000,000-1,999,999	5%
$2,000,000 or more	12%

Actual direct financial losses were less than *potential* losses. Fifty-seven percent of financial professionals report that their organizations did not incur a direct financial loss as a result of fraud activity, while 19 percent report a financial loss of less than $25,000.

Actual Direct Financial Loss from Attempted and/or Actual Payments Fraud in 2018

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

TOTAL DOLLAR AMOUNT	
Zero	57%
Up to $24,999	19%
$25,000-49,999	5%
$50,000-99,999	5%
$100,000-249,999	7%
$250,000-499,999	2%
$500,000-999,999	2%
$1,000,000-1,999,999	–
$2,000,000 or more	2%

Costs to manage/defend and/or clean up from fraud attacks were relatively low for most organizations that experienced such attacks. Forty-two percent of companies did not incur any expenses due to a fraud attempt and 39 percent spent less than $25,000 to defend against or clean up the fraud.

Costs to Manage/Defend/Cleanup from Attempted and/or Actual Payments Fraud in 2018

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

TOTAL DOLLAR AMOUNT	
Zero	42%
Up to $24,999	39%
$25,000-49,999	6%
$50,000-99,999	5%
$100,000-249,999	2%
$250,000-499,999	3%
$500,000-999,999	2%
$1,000,000-1,999,999	1%
$2,000,000 or more	1%

Fraud Costs as a Percentage of Total Revenue

As much of an issue and concern as fraud attacks can be, the impact from payments fraud on a company's bottom line appears to be minimal. Two-thirds of financial professionals report the costs incurred as a result of fraud was half a percent of their organization's annual revenue; 26 percent of companies did not incur a loss.

How Long Did It Take to Discover the Fraud?

Of those organizations that were victims of fraud attacks in 2018, **42 percent detected the fraudulent activity in less than one week**; a mere one percent took one to two years before realizing they had been targeted. As organizations build controls and procedures to guard themselves against these scams, they will also have the ability to quickly detect them and mitigate any damage.

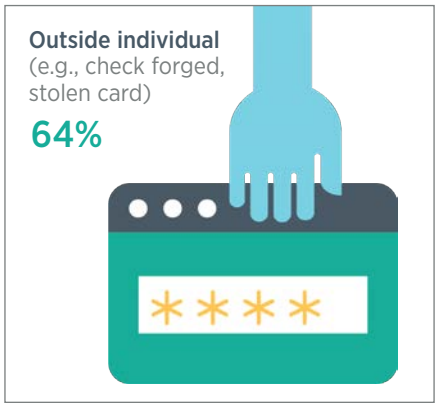
Who Is Responsible for the Payments Fraud Attempt/Attack?

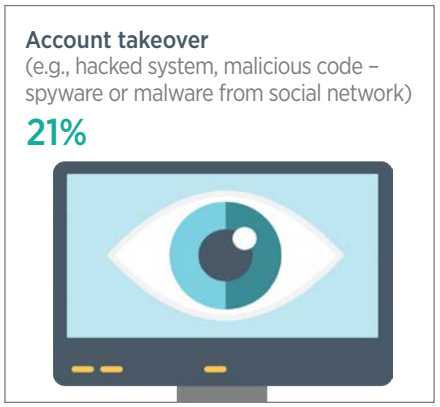
The majority of payments fraud attempts/attacks continues to originate from an external source or individual (e.g., forged check, stolen card). Sixty-four percent of companies that experienced attempted or actual payments fraud in 2018 did so as a result of actions by an individual outside the organization. The second most-common source of payments fraud is Business Email Compromise (BEC) fraud; 58 percent of financial professionals report that payments fraud at their companies originated via BEC. It is particularly concerning that fraud via BEC is on the increase, suggesting perpetrators of these email scams can successfully target their victims.

Other sources of payments fraud include third parties or outsourcers such as a vendor (experienced by 22 percent of organizations—a four-percentage point increase from 2017). Account takeovers (e.g., hacked system, spyware or malware) are reported by 21 percent of companies that experienced attempted/actual payments fraud—an increase from the 13 percent in 2017. These two sources of payments fraud go hand-in-hand with BEC. The significant increase in payments fraud from account takeovers is particularly noteworthy and suggests that instances of phishing in fraud activity via avenues such as BEC are increasing. Fraudsters are successfully "spoofing" legitimate email accounts. This might explain why ACH transactions have been exposed to increased fraud activity. By gaining access to internal systems, fraudsters may successfully be able to generate ACH files.

Fraudsters are aware of the red flags to which organizations are alerting their employees, as well as the training companies are providing to ensure that treasury and finance staff can detect phishing attempts. The recent development of increased "sophisticated" fraud such as account takeovers suggests that fraud mitigation, in addition to robust internal controls, should also focus on network security and how to prevent external parties from gaining access to internal systems.

Sources of Attempted and/or Actual Payments Fraud in 2018
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)





03 BUSINESS EMAIL COMPROMISE

What Is Business Email Compromise?

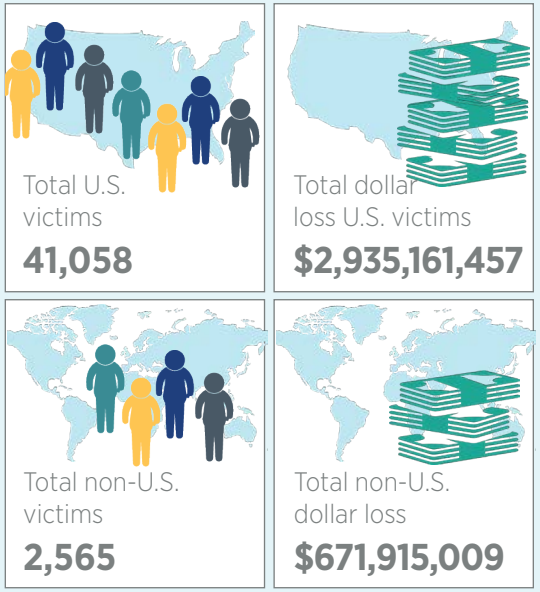
Business Email Compromise (BEC) (also known as Email Account Compromise or EAC) is a sophisticated scam targeting both businesses and individuals initiating who are otherwise responsible for payments. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques in order to conduct unauthorized transfers of funds.

Most victims of BEC/EAC note that wire transfers are a common method of transferring funds for business purposes; however, some report checks are a common payment method targeted by BEC. Fraudsters will use the method most commonly associated with their potential victim's normal business practices. The scam has evolved to include the compromising of legitimate business email accounts, 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 transfers of funds.

Statistical Data

The BEC/EAC scam continues to grow and evolve, targeting small, medium and large businesses as well as personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed dollar losses. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the Internet Crime Compliance Center (IC3) and other financial institutions indicate fraudulent transfers have been sent to 115 countries.

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the Internet Crime Compliance Center (IC3) from October 2013 to May 2018:[1]



Note: Definition and Statistical data shared is from The Federal Bureau of Investigation (FBI)

[1]The Federal Bureau of Investigation (FBI)

Business Email Compromise (BEC) Shows No Signs of Abating

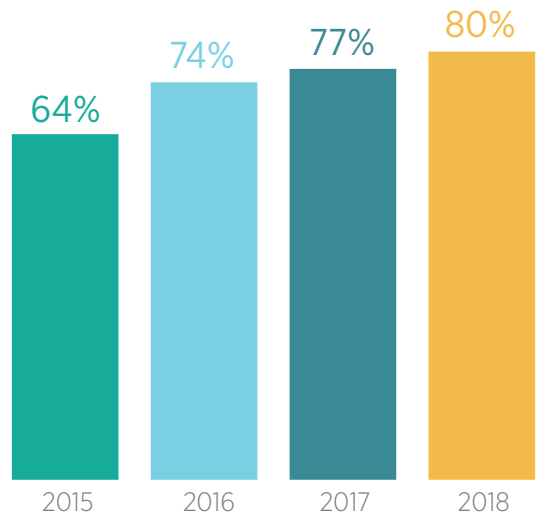
Fraud originating from BEC continues on the uptick. AFP began tracking instances of BEC in 2016 (covering activity for 2015). **The share of companies impacted by BEC has expanded considerably—from 64 percent in 2015 to a solid 80 percent in 2018**. The increase isn't because organizations **don't take notice** of the problem. It's quite the opposite: companies are proactively implementing training for employees so staff are able to recognize fraudulent emails. Scammers, however, are not discouraged and are becoming even more sophisticated in their techniques and can create emails that appear to be authentic.

When individuals do get "scammed" they are exposing their organizations to a variety of risks. Most often the risk involves payments being authorized unknowingly to fraudsters who are often located overseas. Links used in emails can be used to spread malware and spyware and to gain access to organizations' confidential information about their personnel and customers.

Fraudsters use various email tactics to con their victims:

- Posing as senior executives in emails, using spoofed email addresses directing a transfer of funds to fraudsters' accounts (cited by **81 percent** of respondents)
- Impersonating vendors in emails, directing payments (based on authentic invoices) to fraudsters' accounts (**44 percent**)
- Pretending to be other third parties in emails, requesting changes in bank account(s), payments instructions, etc. (**33 percent**)
- Other types of email used in attacks are:
  - Faxes requesting revisions in bank instructions
  - Emails from fraudsters who hacked senior executives and used legitimate outlook accounts
  - Email impersonating HR department, directing employees to sign in to links
  - Emails requesting change in payroll bank information

Percent of Organizations that Experienced Business Email Compromise (BEC), 2015-2018

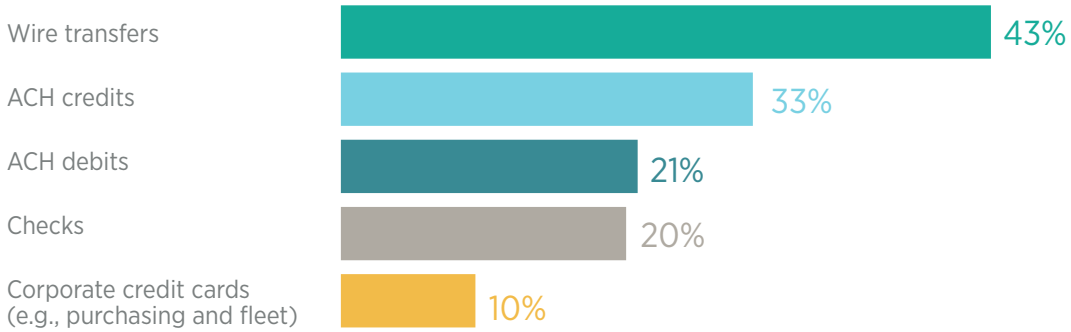


Wire Transfers Are Once Again Prime Targets for Business Email Compromise Scams, and ACH Credits Follow

Forty-three percent of organizations that experienced payments fraud in 2018 did so via BEC that impacted wire transfers. This is a substantial decrease from the 54 percent in 2017 and the 60 percent in 2016. However, wire transfers remain the most favored payment method targeted for fraud via BEC.

One-third of survey respondents report fraudsters accessed ACH credits using BEC. This is a significant increase from the 12 percent that reported the same in last year's survey. The percentage of financial professionals reporting that BEC compromised their organizations' check payments declined—from 34 percent in 2017 to 20 percent in 2018. This is a significant change from results in previous years. The shift to targeting ACH transactions through BEC further supports the notion that fraudsters have managed to gain access to organizations' internal systems through account takeovers and thus able to invade harder-to-reach payment methods.

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



Financial Impact of Business Email Compromise Currently Not Extensive, but on the Uptick

The percentage of financial professionals reporting their companies were victims of BEC has increased, and organizations are highly focused on mitigating such attacks. But while the financial loss incurred at companies as a result of these scams isn't staggering, the share of those impacted is on the rise. **In 2018, 54 percent of organizations were impacted by a financial loss as a result of BEC**, higher than the 46 percent of organizations that were impacted in 2017. The 2019 survey marks the first time since AFP began tracking this data that over half of respondents report experiencing actual losses from BEC.

Forty-nine percent of smaller organizations (annual revenue less than $1 billion) incurred losses from BEC—a share unchanged from last year—while 57 percent of larger organizations (annual revenue of at least $1 billion) had losses as a result of BEC, an increase from the 46 percent last year. This is a shift from the results in the *2018 Payments Fraud Survey* (data for 2017) in which smaller organizations were more likely to have suffered losses.

There are, of course, other "losses" that can result from BEC. If a fraud attack via BEC exposes personal and confidential information, the nonfinancial damages, while difficult to quantify, can be severe. A greater share of larger organizations (annual revenue of at least $1 billion) and with more than 100 payment accounts were financially impacted by BEC in 2018 (64 percent) than were other companies; 25 percent of respondents from this group report their companies incurred a loss of $1 million or more as a result of BEC. This result clearly demonstrates that fraudsters are targeting larger organizations hoping to steal larger amounts of money.

Aside from this development, the dollar ranges of actual financial loss due to BEC have not changed dramatically over the past couple of years. This again indicates that the scams are tailored so as not to raise any red flags—i.e., by requesting transfers of amounts that are not out of the ordinary.

Estimated Total Dollar Loss to Organization from BEC in 2018
(Percentage Distribution of Organizations that Experienced Payments Fraud via BEC)

TOTAL DOLLAR AMOUNT	
Zero	46%
Up to $24,999	10%
$25,000-49,999	8%
$50,000-99,999	8%
$100,000-249,999	9%
$250,000-499,999	6%
$500,000-999,999	3%
$1,000,000-1,999,999	3%
$2,000,000 or more	8%

04 PAYMENTS FRAUD CONTROLS

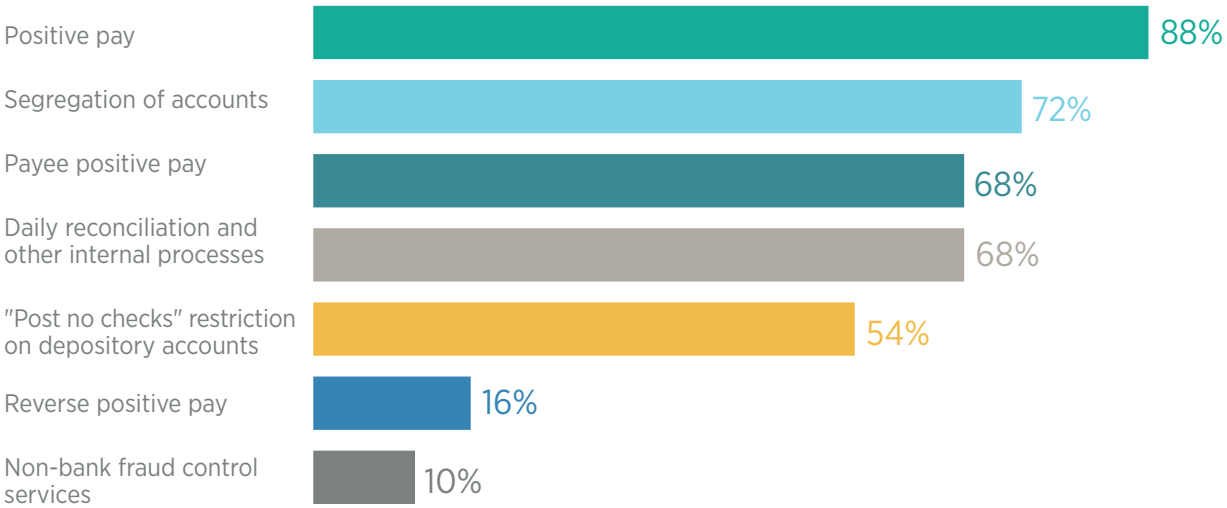
Positive Pay and Segregation of Accounts Are Most Frequently Used Procedures to Protect Against Check Fraud

Positive pay continues to be the method most often used by organizations to guard against check fraud. This approach is used by 88 percent of organizations—similar to the 90 percent reported for 2017. Protective measures such as Positive Pay are not generally included in the payment offering from the financial institution but an added service that charges an extra fee. This can explain the fluctuating use of Positive Pay from previous years. **A slightly larger share of organizations resorts to segregation of accounts (72 percent) than the share that reported the same in last year's survey (68 percent)**.

Other prevalent methods being used to guard against check fraud are:

- Daily reconciliations and other internal processes (cited by **68 percent** of respondents)
- Payee positive pay (**68 percent**)
- "Post no checks" restriction on depository accounts (**54 percent**)

Fraud Control Procedures and Services Used to Protect Against Check Fraud
(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)



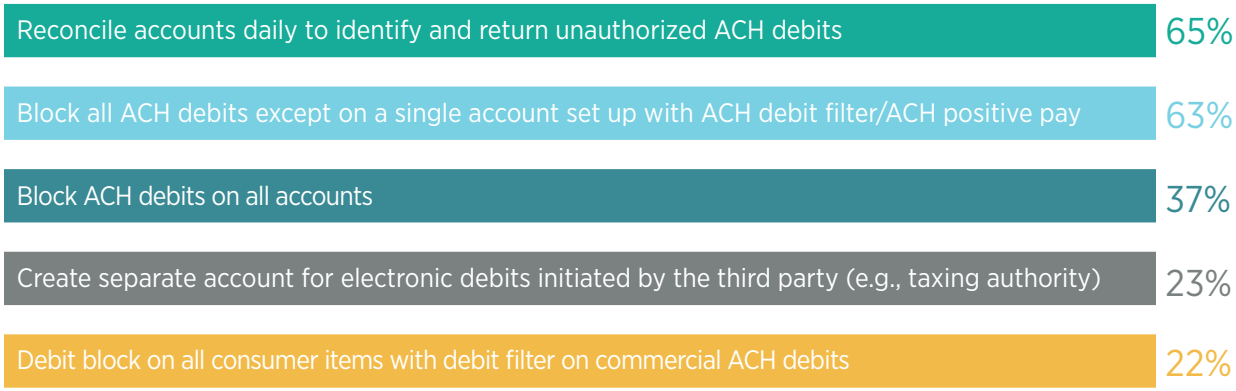
Controlling ACH Fraud

In 2018, 33 percent of organizations were subject to ACH debit fraud and 20 percent were subject to ACH credit fraud. The share of companies exposed to payments fraud via ACH debit and ACH credit increased from 28 percent (ACH debit) and 13 percent (ACH credit), respectively, in 2017. Compared to last year's survey results, ACH is the only payment method that experienced an increase in payments fraud (fraud via checks and wire transfers declined).

To limit the occurrence of ACH fraud, companies are implementing various measures:

- Reconciling accounts daily to identify and return unauthorized ACH debits, cited by **65 percent** of survey respondents for **2018**—a decrease from **69 percent** in **2017**
- Block all ACH debits except on a single account set up with ACH debit filter/ACH positive pay (**63 percent**)—a slight increase from **60 percent** in **2017**
- Block ACH debits on all accounts (**37 percent**)—again, a slight decrease from **35 percent** a **year ago**

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



Mitigating Potential Additional Risks with Same-Day ACH Operational for Both Credit and Debit Transactions

While Same-Day ACH is operational for both credit and debit transactions, 56 percent of organizations are not actively taking steps to prepare and mitigate additional risks that might arise. In addition, 30 percent of financial professionals report that their organizations have no plans to make any revisions to prevent additional risks; over one-fourth of respondents indicates they have not received any advice from their banks. Smaller shares of companies are preparing to guard against any additional risks that might arise; 18 percent of survey respondents indicate their organizations have implemented various plans to mitigate potential additional risks, and 23 percent report their companies are in the process of doing so.

Financial Professionals Are Preparing to Guard against Email Scams

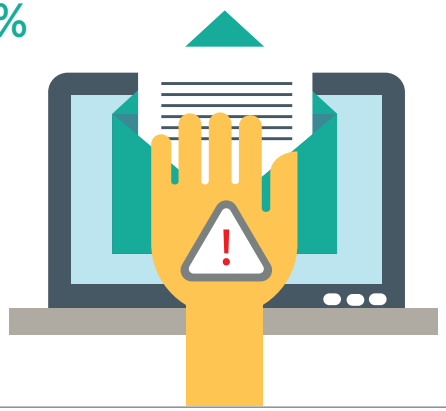
To guard against BEC, companies are implementing various procedures to prevent their employees from being "scammed" by fraudulent emails. Some are focused on raising employee awareness of scam emails and training them to better detect these phishing alerts. **Over three-fourths of companies are adopting stronger internal controls that prohibit initiation of payments based on emails or other, less secure messaging systems.** Seventy-six percent of organizations are educating their staff about the threat of BEC and how to recognize phishing attempts.

Other controls being implemented are:

- Implementing company policies for providing appropriate verification of any changes to existing invoices, bank deposit information and contact information (cited by **68 percent** of respondents)
- Adopting a two-factor (at least) authentication or other added layers of security for access to company network and payments initiation (**65 percent**)
- Confirming requests for transfer of funds by using phone verification as part of a two-factor authentication (**51 percent**)
- An intrusion detecting system that flags emails with extensions that are similar to company email (**30 percent**)

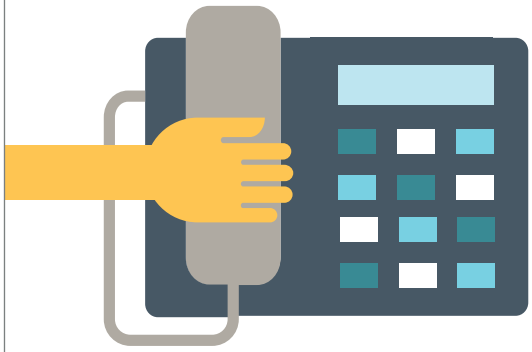
Stronger Internal Controls prohibiting payments initiation based on emails or other less secure messaging systems

76%



Education and training on the BEC threat and how to identify phishing attempts

76%



Implementing company policies for providing appropriate verification

68%

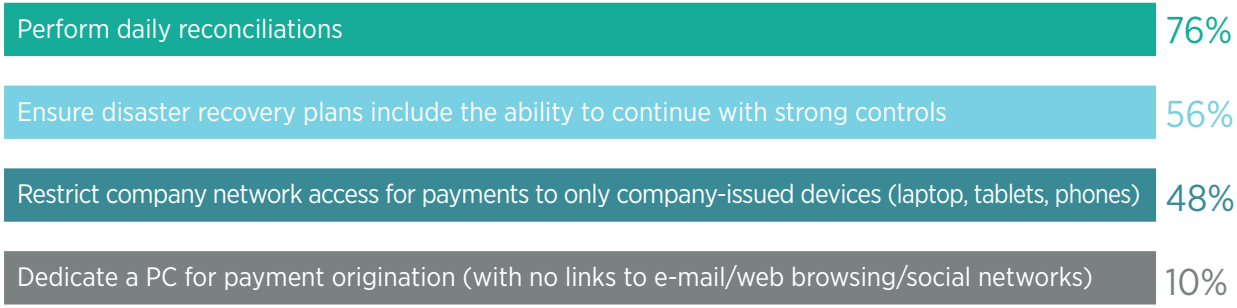
Adopted at least a two-factor authentication or other added layers of security

65%

Defending Against Attacks on Security Credentials

In trying to protect their payment methods from attacks on security credentials, a large majority of organizations performs daily reconciliations (cited by 76 percent of respondents). Over half are planning for disaster recovery (56 percent) and 48 percent restrict company network access to only company-issued devices (laptop, tablets, phones).

Measures Taken by Organizations to Defend Against Attacks on Security Credentials
(Percent of Organizations that Experienced Attempted or Actual Payments Fraud)



Conclusion

After a period of declining payments fraud activity, there has been a sharp increase in the past few years. Financial practitioners are not expecting any change in this trend, and are equipping their organizations to better manage the perils associated with fraud activity, making significant efforts to implement measures that will restrict fraudsters' success. **Organizations and their treasury/finance staff cannot afford to be complacent; they all must be vigilant**. Fraudsters seek to attack targets that lack protection. While not every organization can protect itself completely, having a variety of protective measures in place will likely frustrate fraudsters and they'll move on to easier targets.

Technology will likely be used by perpetrators to commit crimes and inflict extensive damage; fraudsters keep up to date with new technology and are constantly finding new schemes to capture funds from their targets. But while new technology can be fraudsters' favorite tool, it can also be used by organizations in helping prevent hacks into payment systems.

Notably, fraud committed via BEC is also increasing; 80 percent of organizations were targets of compromised emails leading to payments fraud in 2018. In addition, the share of organizations that suffered actual financial losses from such schemes rose for the first time since AFP began tracking payments fraud. Over half of those companies impacted by BEC incurred a financial loss, indicating the perpetrators of these attacks were successful in scamming employees at the organizations. These results also highlight the fact that BEC fraud is evolving, with fraudsters utilizing this avenue to successfully cheat their targets into sending funds to "fake" recipients. The techniques being used are sophisticated and company employees are not always able to detect the scam.

There has been a significant increase in ACH fraud. Over the past decade there has been a slight increase in ACH credit fraud—from four percent to 13 percent—suggesting a moderately heightened risk of fraud via this payment method, although survey results reveal no real reasons behind the increase. That changed significantly in 2018: the percentage of organizations experiencing fraud via ACH credit increased seven percentage points from 2017 to 20 percent in 2018. Fraud via ACH debits also increased—from 28 percent in 2017 to 33 percent in 2018. ACH transactions have also become much more popular as the targeted payment method for BEC scams, while fraud via wire transfers and checks has declined.

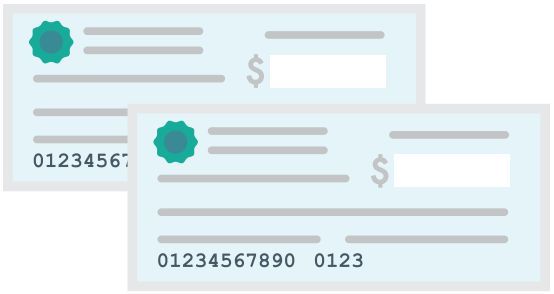
It is encouraging that financial leaders are actively implementing controls to prevent their organizations from being vulnerable targets for payments fraud.

But as the share of companies encountering payments fraud continues to rise, they may not be cognizant of what is required to prevent such attacks. Of particular concern is the increased threat of phishing which could facilitate account takeovers and access to internal networks.

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

Key Highlights:

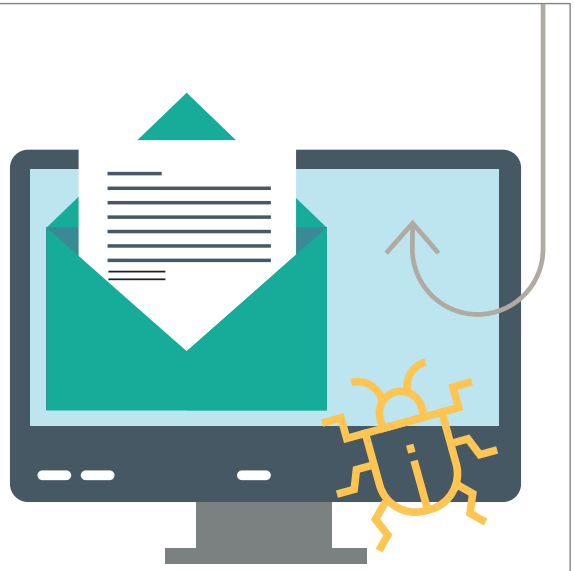
In the past five years **payments fraud activity has increased dramatically**. A significant 82 percent of financial professionals report that their organizations experienced attempted and/or actual payments fraud in 2018, 20 percentage points higher than reported in 2014.



While checks continue to be the payment method most impacted by fraud activity in 2018, **the percentage of financial professionals reporting check fraud activity decreased from 2017 to 2018**.

Fraud via ACH debits and ACH credits increased; checks, wire transfers and cards all saw declines.

Fraud originating from BEC continues to be on the uptick. AFP began tracking instances of BEC in 2016; the percentage of companies impacted by BEC since has risen considerably from 64 percent in 2015 to 80 percent in 2018.



Even though the percentage of companies that are victims of BEC is on the rise, and despite the fact that organizations are highly focused on mitigating these attacks, **the financial loss incurred at companies as a result of these scams—while not staggering—is nevertheless on the increase**. In 2018, 54 percent of organizations were impacted by a financial loss as a result of BEC (an increase of eight percent over 2017) and the first time more than half of the respondents reported estimated losses from these scams.

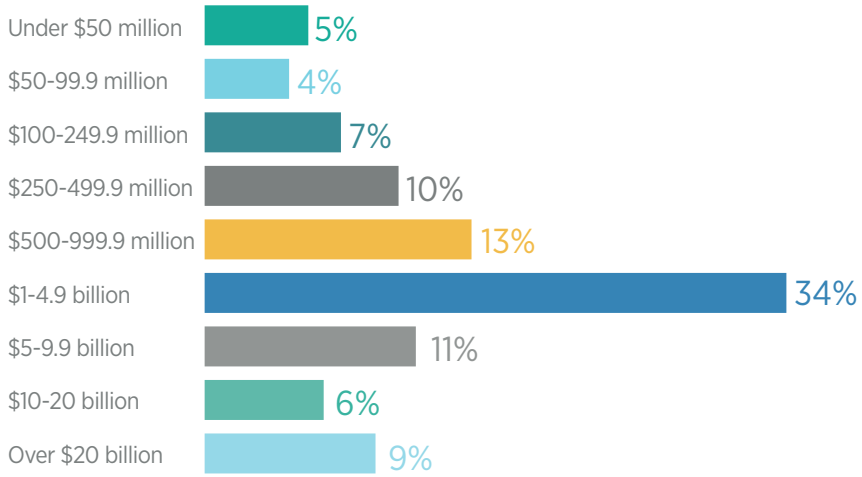
05 ABOUT SURVEY PARTICIPANTS

About the Survey Participants

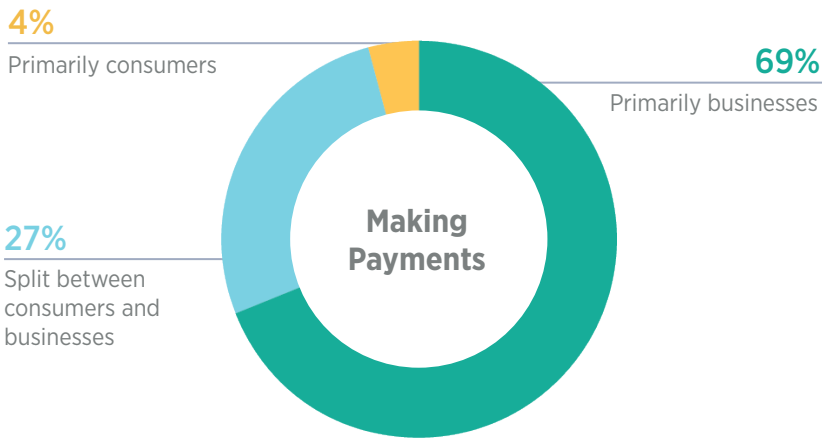
In January 2019, the Research Department of the Association for Financial Professionals® (AFP) surveyed nearly 10,000 of its corporate practitioner members and prospects. The survey was sent to corporate practitioners with the following job titles: cash manager, treasurer, assistant treasurer, analyst, director, and vice president of treasury. We received 417 responses from members and an additional 200 responses from prospects, generating a total of 617 responses.

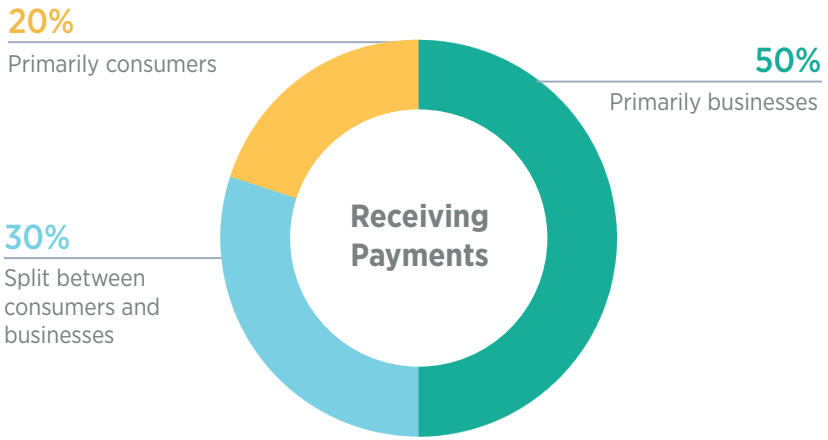
AFP thanks J.P. Morgan for underwriting the *2019 AFP Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. The following tables provide a profile of the survey respondents, including payment types used and accepted.

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



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



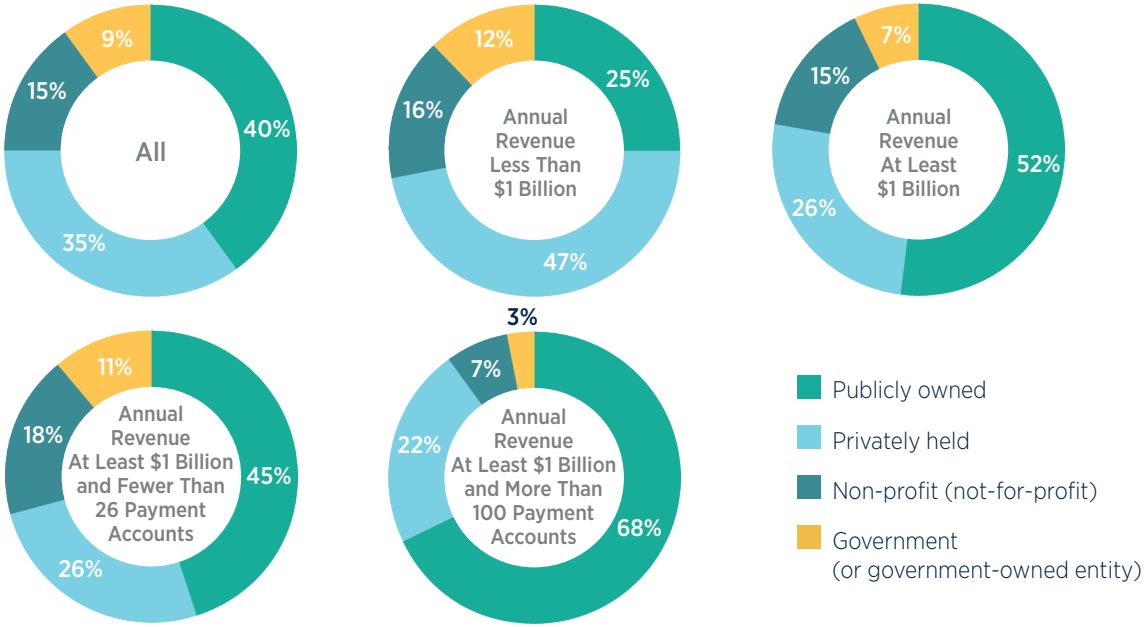


About the Survey Participants continued

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	22%	31%	17%	32%	–
5-9	20%	20%	21%	38%	–
10-25	18%	17%	16%	30%	–
26-50	12%	11%	14%	–	–
51-100	8%	9%	7%	–	–
More than 100	21%	12%	25%	–	100%

Organization's Ownership Type
(Percentage Distribution of Organizations)



Industry
(Percentage Distribution of Organizations)

	ALL
Administrative Support/Business services/Consulting	2%
Banking/Financial services	9%
Construction	1%
Energy	5%
Government	7%
Health Care and Social Assistance	8%
Hospitality/Travel/Food Services	2%
Insurance	7%
Manufacturing	19%
Non-profit	7%
Petroleum	2%
Professional/Scientific/Technical Services	2%
Real Estate/Rental/Leasing	5%
Retail Trade	5%
Wholesale Distribution	3%
Software/Technology	4%
Telecommunications/Media	2%
Transportation and Warehousing	4%
Utilities	4%

AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. AFP Research draws on the knowledge of the Association's members and its subject matter experts in areas that include bank relationship management, risk management, payments, 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

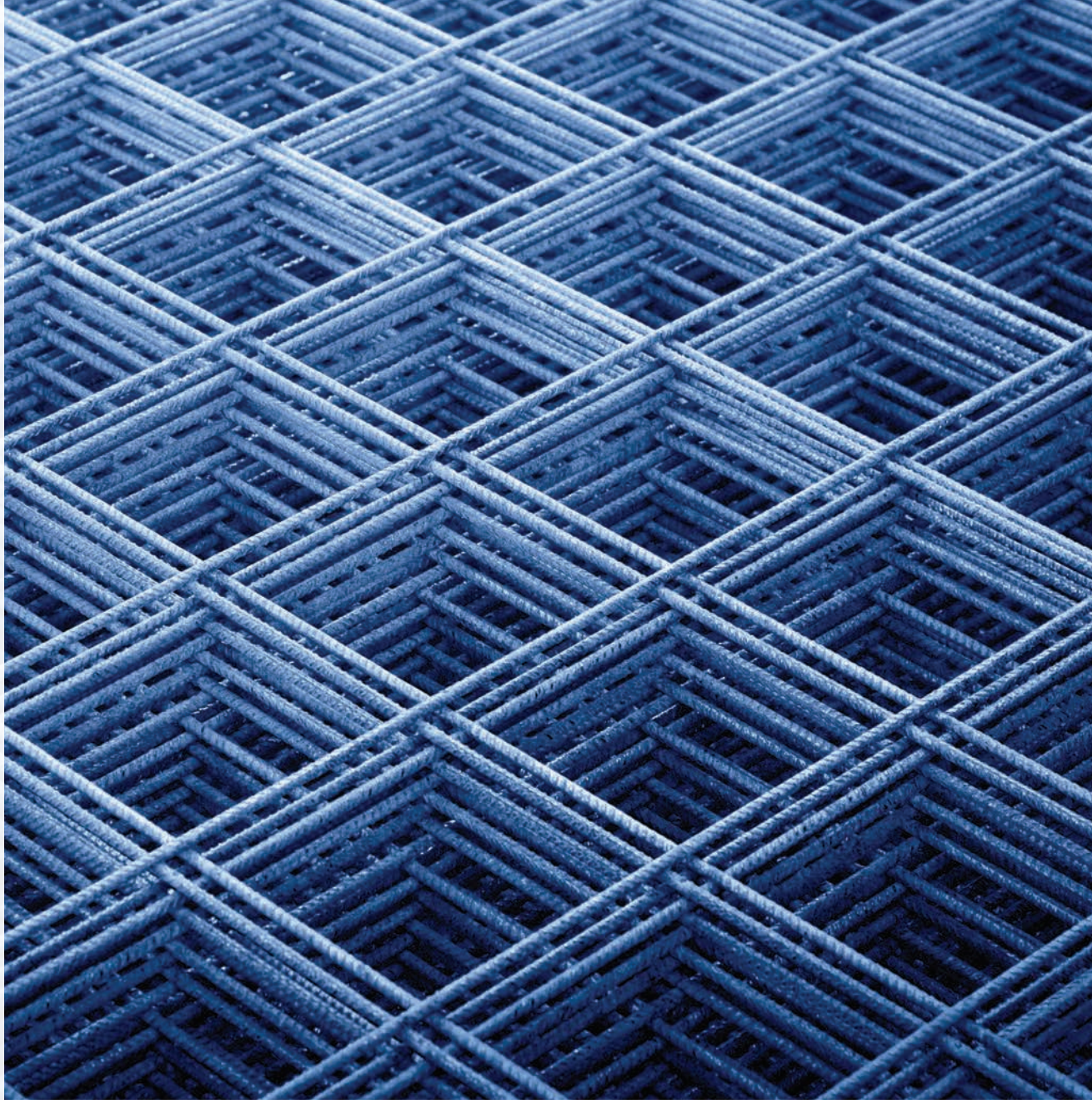
J.P. Morgan is proud to sponsor the 2019 AFP Payments Fraud & Control Survey.

In 2018, 82 percent of organizations reported incidents of fraud and 43 percent experienced direct financial loss as a result.

We are committed to fraud mitigation and information protection across our infrastructure—and continue to invest in technology, tools and risk management expertise.

Visit our Fraud Resource Center to learn more about trends and best practices for safeguarding your business.

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



J.P.Morgan