ASSOCIATION FOR FINANCIAL PROFESSIONALS

2015 AFP

Payments Fraud and Control Survey

REPORT OF SURVEY RESULTS

Underwritten by

J.P.Morgan

2015 AFP

Payments Fraud and Control Survey

REPORT OF SURVEY RESULTS

March 2015

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

J.P. Morgan is proud to once again sponsor the AFP® Payments Fraud and Control Survey for the seventh consecutive year and we are pleased to provide you with a complimentary copy of AFP's 2015 report. The survey results show that now, more than ever, the need for new cyber security models and strict control governance is crucial for all businesses given that 62 percent of companies were targets of payments fraud last year.

Some of the key findings in this year's survey include:

- 92 percent of finance professionals believe EMV (EuroPay, MasterCard and Visa) cards will be effective in reducing point-of-sale (POS) fraud
- 61 percent believe that chip-and-PIN will be the most effective authentication method in mitigating credit/debit card payments fraud
- Wires fraud incidents nearly doubled, from 14 percent in 2013 to 27 percent last year
- Paper checks continue to lead as the payment type most susceptible to fraudulent attacks even as their overall use continues to decline
- Credit and debit cards experienced a decline in fraudulent activity, down from 43% in 2013 to 34% in 2014

With these statistics in mind, it is important for all businesses to take preventive measures to prevent cyber fraud by educating their employees on current payments fraud practices and implementing the products and processes they need to protect their corporate assets.

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

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 cyber security protection protocols.

With best regards,

Nancy K. McDonnell
Managing Director
J.P. Morgan

Introduction

In 2014 the incidents of payments fraud were rampant nationwide. While those perpetrators committing payments fraud seemed to focus especially on high-profile retailers, breaches of payments systems impacted companies of all sizes and in a variety of industries. As technology begins to play a more dominant role in the payments arena, we are going to witness more instances of cyberfraud attempts.

Finance professionals at these organizations are tasked with dealing with the aftermath of payments fraud attacks. That effort includes the possible remediation of their companies' reputation with investors and customers as well as restoring the confidence of consumers whose personal data have often been compromised in the wake of such data breaches. These professionals must also remain vigilant as affected companies may suffer from direct hits to their bottom lines.

Preventing and defending against payments fraud is challenging, especially as methods of committing payments fraud have and continue to become extremely sophisticated and are constantly evolving. Against this backdrop, it is imperative that organizations implement security features to guard against any possible payments fraud.

Finance professionals are at the forefront of payments fraud defense. They use a large body of knowledge and a variety of tools to guard their organizations from such attacks. Still, it is evident that not all efforts have been fully successful in countering the activities of malicious fraudsters.

To gauge the trends and the challenges associated with payments fraud, the Association for Financial Professionals® (AFP) has conducted surveys each year since 2005. Those surveys examine the nature and frequency of fraudulent attacks on business-to-business payments and how organizations prepare themselves to deal with fraud. Continuing those efforts, AFP conducted its 11th annual Payments Fraud and Control Survey in January 2015. Results of the survey are reflected in the *2015 AFP Payments Fraud and Control Survey Report.*

Key highlights from this survey report include:

- **Sixty-two percent** of companies were subject to payments fraud in 2014.
- **Checks** remain the most-often targeted payment method by those committing fraud attacks. Check fraud also accounts for the largest dollar amount of financial loss due to fraud.
- **Credit/debit cards** are the second most frequent targets of payments fraud.
- **A vast majority of survey respondents** (92 percent) firmly believe EMV-enabled credit/debit cards will be effective in reducing point-of-sale (POS) fraud.
- **Sixty-one percent** of survey respondents report that Chip-and-PIN validation will be most effective in preventing credit/debit card fraud.

AFP thanks J.P. Morgan for its long-time and continued underwriting support of AFP's payments fraud survey series. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibilities of the AFP Research Department. Information on the survey methodology can be found at the end of this report.

KEY FINDINGS

ASSOCIATION FOR FINANCIAL PROFESSIONALS

2015 AFP

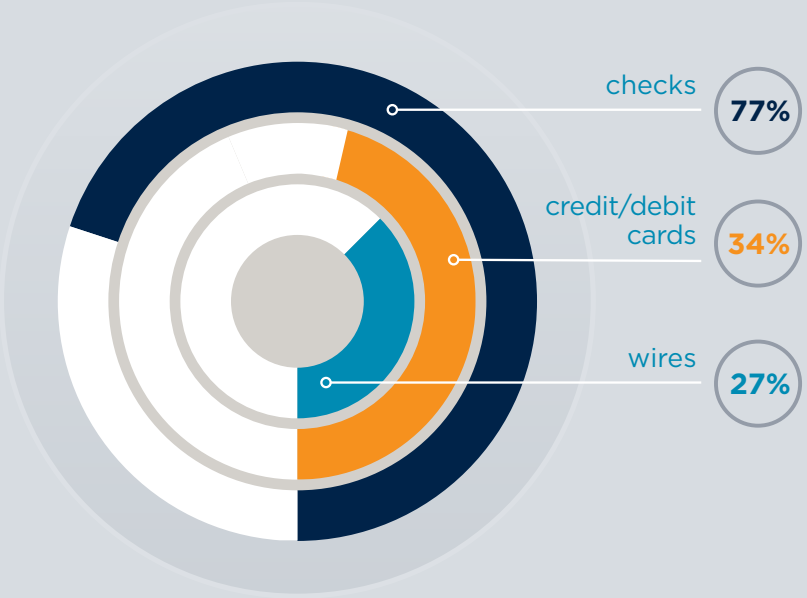
Payments Fraud and Control Survey

Underwritten by J.P.Morgan

62%

of companies were targets of payments fraud in 2014.

MOST TARGETED METHODS



92%

of professionals firmly believe EMV cards will be effective in reducing POS fraud.

Payments Fraud Overview

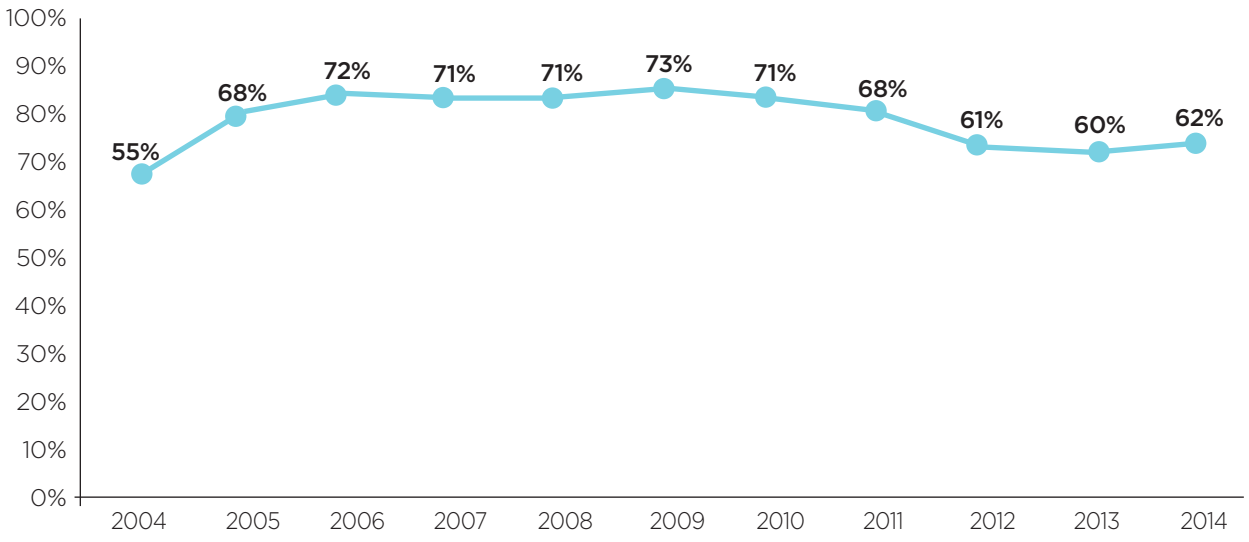
The payments sector is rapidly evolving. Also, not surprisingly, is payments fraud. As new payment methods enter the marketplace so too do new and enterprising criminal attempts of exploiting any weaknesses in those systems.

The potential access to funds and sensitive personal and financial information makes payment methods very attractive targets for fraudsters. While technology improvements can often be useful tools in assisting criminals in perpetrating fraud, if used to their fullest extent those same technology enhancements can play an important role in preventing fraud.

Sixty-two percent of finance professionals report that their organizations were targets of payments fraud in 2014. That is a slight increase compared to the incidence of fraud in the two previous years. It does, however, represent an 11-percentage-point *decline* from 2009: 73 percent of companies—the largest percentage on record—were subject to attempted or actual payments fraud five years ago during the midst of the last recession.

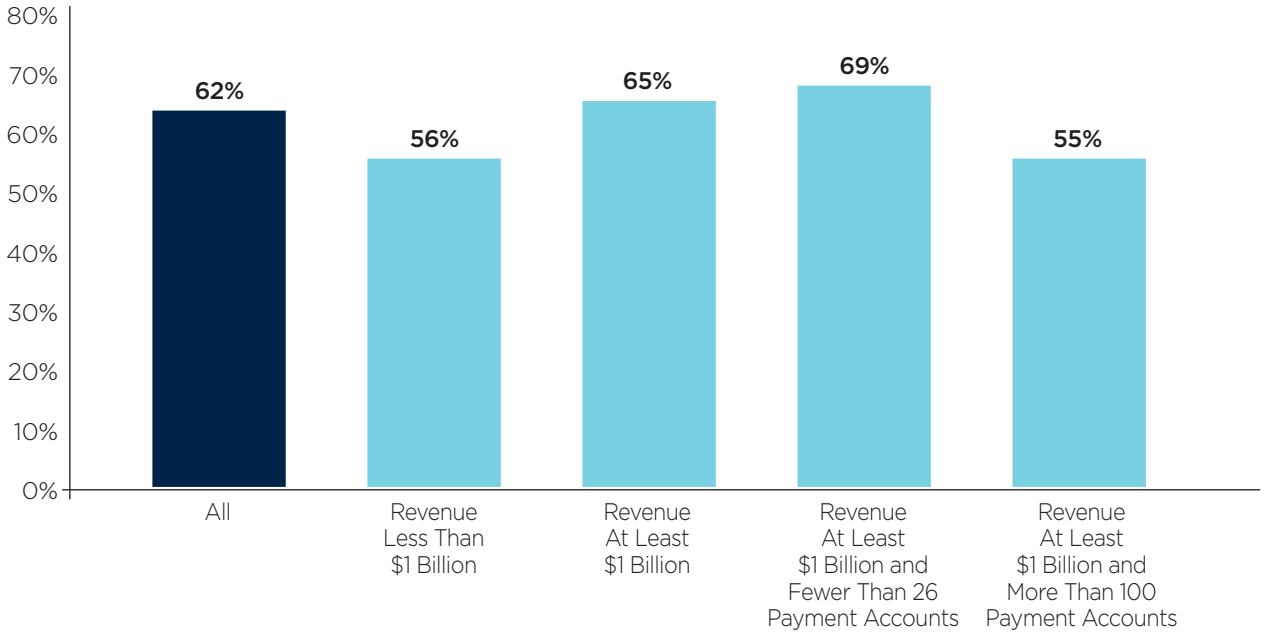
62%
of companies, were targets of payments fraud in 2014

Percent of Organizations Subject to Attempted and/or Actual Payments



Large organizations are more likely to have been subject to actual and/or attempted payments fraud than are smaller companies. Sixty-five percent of organizations with annual revenues of at least $1 billion were victims of payments fraud in 2014 compared to 56 percent of companies reporting annual revenues of less than $1 billion.

Percent of Organizations Subject to Attempted and/or Actual Payments Fraud in 2014



Checks continue to be the payment method most often targeted by those committing (or attempting to commit) payments fraud. Seventy-seven percent of organizations that experienced attempted or actual payments fraud in 2014 were victims of check fraud. This is a decrease from the 82 percent that suffered check fraud in 2013 and could be attributed to the decline in check use at many organizations. While their use has, indeed, gradually declined in recent years, checks continue to account for 50 percent of business-to-business (B2B) payments in the U.S.[1]

There are two primary reasons why checks continue to be the payment method of choice. One, organizations' business partners are hesitant to switch to electronic payments. Secondly, those partners are often unwilling to share their bank information. Despite these challenges, the use of checks is expected to continue to decline with the increasing popularity of more efficient payment methods.

The second most popular vehicle for payments fraud is corporate and commercial credit/debit cards. A third of finance professionals (34 percent) whose organizations were exposed to payments fraud in 2014 report that such fraud attempts were via credit/debit cards. Another 27 percent of survey respondents indicate their companies experienced wire transfer fraud. That is a significant increase from the 14 percent that reported wire transfer fraud in 2013. Following closely behind: is ACH debits (cited by 25 percent of respondents).

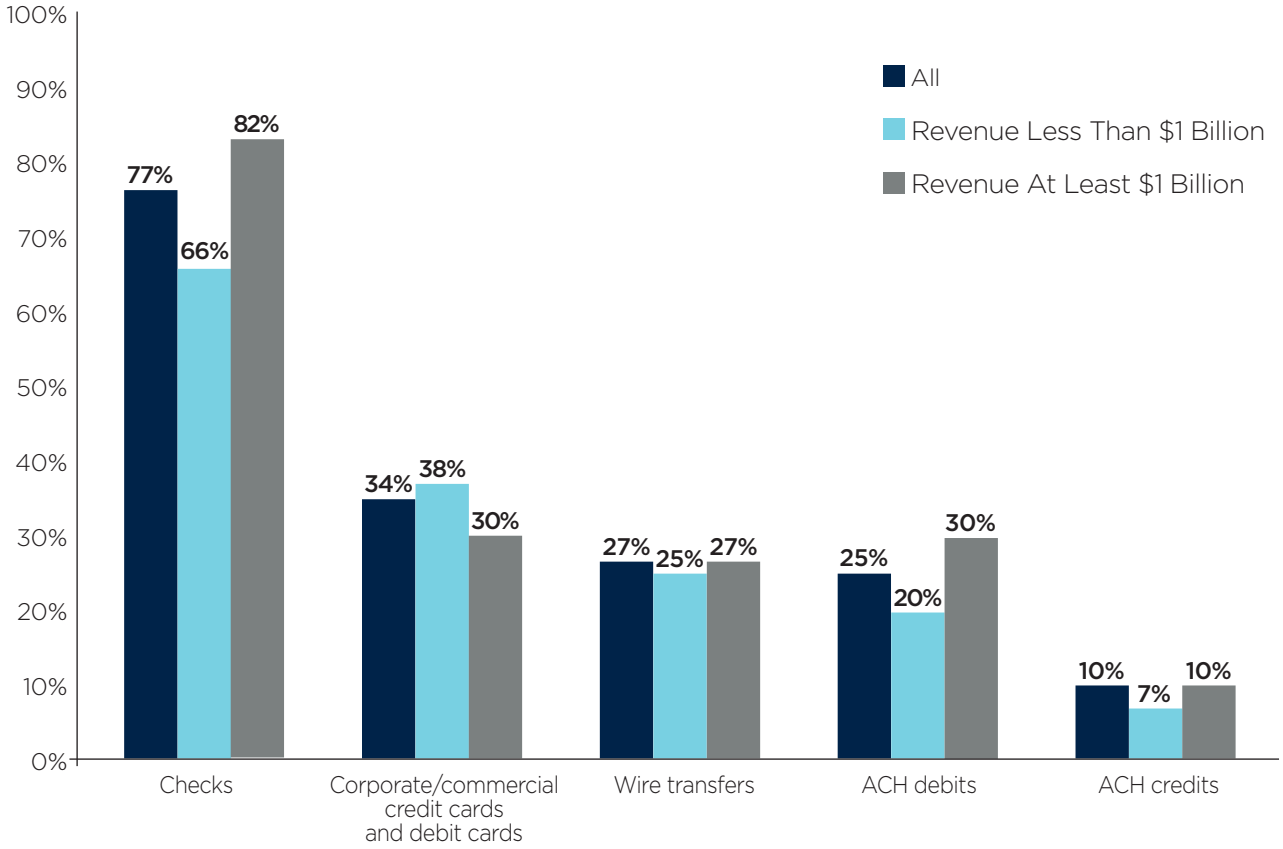
Checks continue to be the payment method most often targeted by those committing payment fraud

77% of organizations subject to payments fraud in 2014 were victims of check fraud

1. *2013 AFP Electronic Payments Survey*

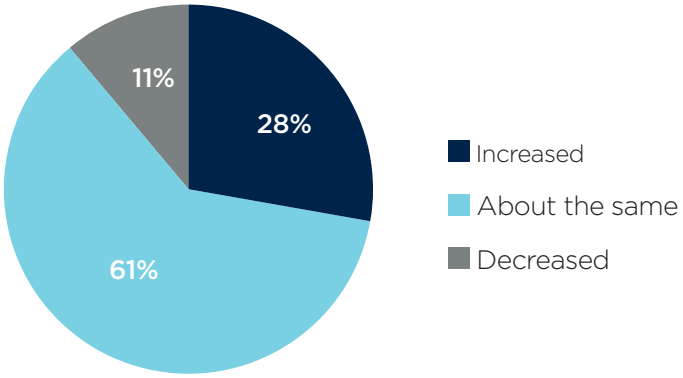
Given the numerous data breaches experienced in 2014, an increase in fraud attempts overall was expected. But the reported increase in wire fraud during 2014 is a little surprising; it may reflect fraudsters "shifting their focus" to organizations' accounts payable departments. Fraudsters are resorting to cyberfraud tactics and are conducting research on and creating profiles of company executives, then attempting to send emails with payment instructions to A/P employees that appear to be from the company's CEO or CFO. In this scenario, email addresses may be hacked, or slightly altered, to deceive the employee into complying and making the payment. Fraudsters may also pose as vendors and request that their payment information be changed because of a new bank relationship, etc.

Payment Method Subject to Attempted or Actual Payments Fraud in 2014
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)



While the incidence of payments fraud was unchanged at most companies, over a quarter of organizations experienced an increase in payments fraud attacks in 2014. Twenty-eight percent of survey respondents whose organizations experienced payments fraud report that the number of incidents of fraud attempts increased in 2014 compared to 2013. Eleven percent indicate the number of instances declined while a majority (61 percent) report the incidents of payments fraud at their organizations remained unchanged from 2013.

Change in Prevalence of Payments Fraud in 2014 Compared to 2013
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)



Finance professionals from smaller companies—those with annual revenues of less than $1 billion—report a 32 percent increase in fraud incidence in 2014 compared to that in 2013. Survey respondents from larger companies report a 26 percent increase in the incidents of fraud year over year. Sixty-five percent of corporate practitioners from larger-sized organizations report that the instances of fraud in 2014 were relatively unchanged from 2013.

Financial Loss from Fraud Attempts

In most cases, the potential loss to a company from an attempted payments fraud attack resulted in a relatively small financial loss. For 39 percent of organizations, the potential loss from fraud in 2014 is estimated to be less than $25,000; for 31 percent of organizations the potential loss is between $25,000-249,999. The potential loss is $250,000 or more at 19 percent of organizations.

Large organizations with over 100 payment accounts are more likely than other companies to have experienced potential loss in the highest dollar ranges. Twenty-eight percent of finance professionals from these companies report the potential loss from fraud in 2014 was greater than $250,000.

Potential Financial Loss from Attempted or Actual Payments Fraud in 2014
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Zero				
11%	11%	10%	9%	12%
Up to $24,999				
38	46	34	36	37
$25,000-49,999				
10	11	11	12	–
$50,000-99,999				
11	13	10	8	12
$100,000-249,999				
10	6	14	15	12
$250,000 and above				
19	13	22	19	28

Most organizations that were subject to at least one payments fraud attempt in 2014 did not suffer any *actual* financial loss resulting from the fraud. Seventy percent of organizations that were subject to at least one payments fraud attempt in 2014 did not incur actual losses from the attempt. Eighteen percent realized a financial loss of less than $25,000 while four percent of survey respondents report a loss to their organizations in excess of $250,000. Again, larger organizations with a greater number of payment accounts are more likely to have experienced direct financial losses; 12 percent of such companies suffered a financial loss exceeding $250,000. The typical financial loss incurred by companies due to payments fraud in 2014 was $20,000.

70% of companies that were subject to payments fraud in 2014 did not suffer a financial loss from the attack

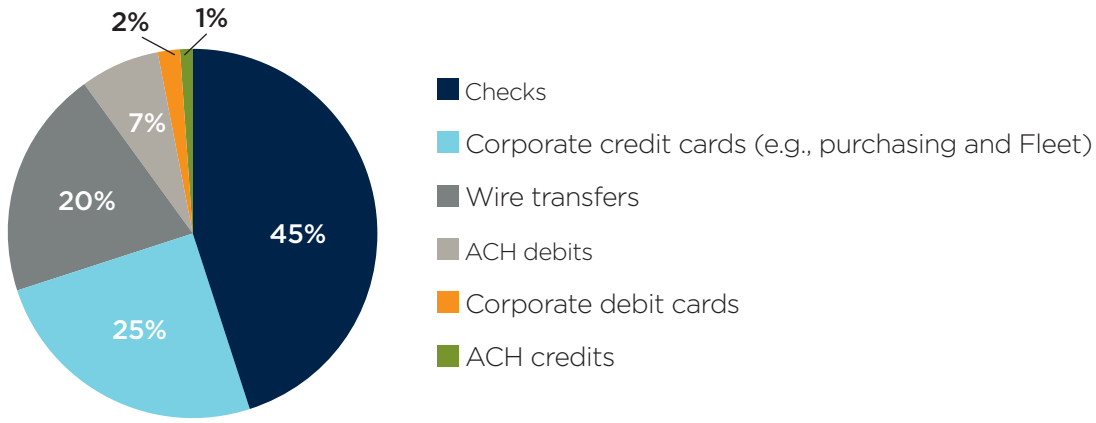
Actual Direct Financial Loss from Attempted or Actual Payments Fraud in 2014
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Zero				
70%	71%	71%	78%	52%
Up to $24,999				
18	22	14	15	17
$25,000-49,999				
3	3	3	2	2
$50,000-99,999				
3	1	3	1	7
$100,000-249,999				
3	2	4	1	10
$250,000 and above				
4	1	5	4	12

Not only are checks the payment method most often targeted by fraudsters. In 2014, they also continued (as in previous years) to be the payment method accounting for the largest dollar amount of loss due to fraud. Yet, the percentage of organizations that suffered financial loss as a result of such fraud declined—from 57 percent in 2013 to 45 percent in 2014. Fraudulent use of corporate cards was responsible for 25 percent of actual financial loss, close to the 23 percent reported in 2013. Two-thirds of survey respondents from larger organizations with fewer than 26 payment accounts report that the greatest financial loss was a result of fraud perpetrated on payment methods other than checks.

Checks continue to account for the largest dollar amount of loss due to payments fraud

Payment Method Responsible for Largest Dollar Amount of Fraud Loss
(Percentage Distribution of Organizations that Suffered Financial Loss from Payments Fraud)



For most organizations that were subject to attempted or actual payments fraud in 2014, the costs to manage/defend and/or "clean up" from the events was relatively low. Slightly less than half (46 percent) the organizations did not incur any expenses as a result of fraud and 41 percent spent less than $25,000 to defend against or clean up the fraud. Larger organizations—particularly those with a greater number of payment accounts—are more likely to have spent larger amounts on cleaning up and defending against fraud than are other companies.

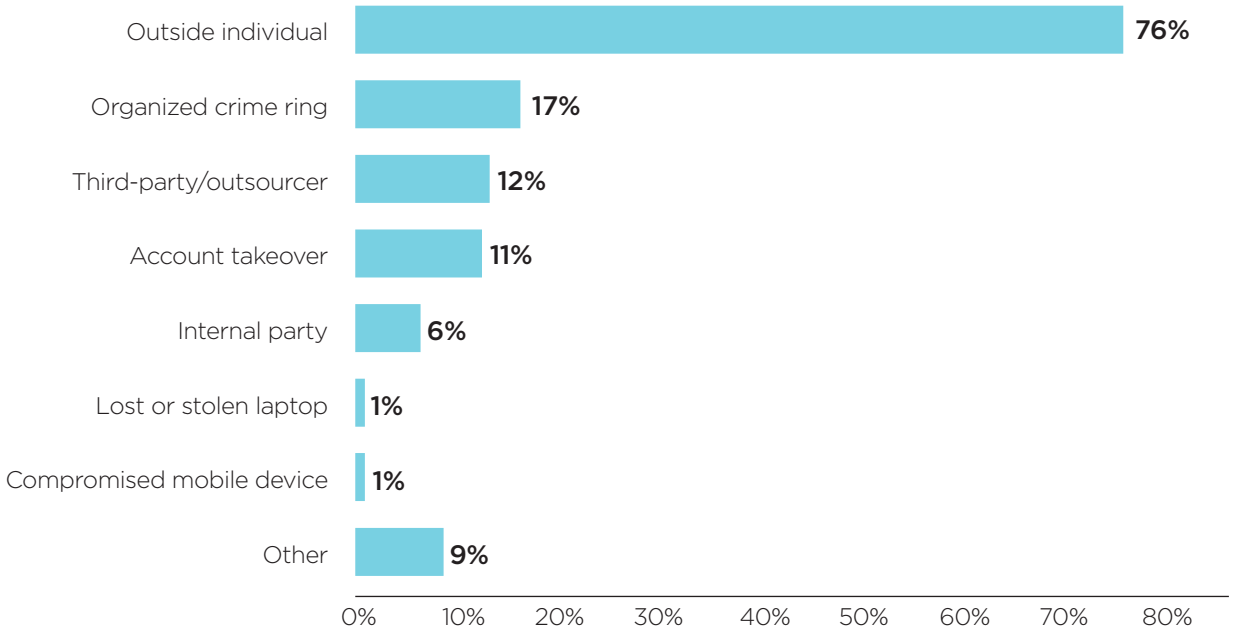
Costs to Manage/Defend/Clean Up Payments Fraud in 2014
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Zero				
46%	46%	47%	55%	33%
Up to $24,999				
41	46	36	34	38
$25,000-49,999				
4	4	4	4	7
$50,000-99,999				
5	2	6	5	5
$100,000-249,999				
2	1	3	1	5
$250,000 and above				
3	1	4	2	12

The majority of payments fraud originates from outside an organization. Three-fourths (76 percent) of organizations that experienced attempted or actual payments fraud in 2014 did so as a result of actions by an outside individual. For 17 percent of companies, payments fraud originated from an organized crime ring and 12 percent of organizations were subject to fraud from a third party or outsourcer.

Outside individuals are the source of payments fraud attacks at **3/4ths** of organizations

Sources of Attempt/Actual Payments Fraud in 2014
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)



Check Fraud

As reported earlier, checks are the payment method most often subject to fraudulent activity. Fifty-six percent of organizations experienced between one and five incidents of check fraud in 2014 while 17 percent were subject to between six and ten incidents. The share of organizations exposed to at least 20 check fraud attempts in 2014 was 17 percent—a significant decrease from the 27 percent in 2013. Larger companies with more than 100 payments accounts are more likely to have experienced check fraud more frequently than other companies; 43 percent of finance professionals from this cohort report their organizations were exposed to check fraud more than 15 times. Nearly three-fourths of survey respondents (72 percent) report that the number of check fraud attempts in 2014 was unchanged from that in 2013 while 19 percent report an increase.

Number of Times Organization Experienced Attempted or Actual Check Fraud in 2014
(Percentage Distribution of Organizations that Suffered at Least One Attempt of Check Fraud)

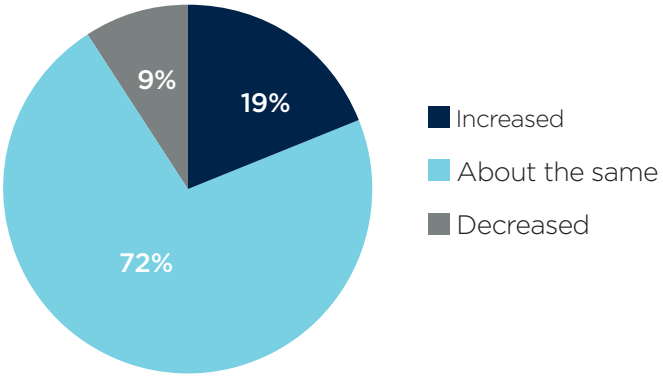
All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
1-5 56%	68%	46%	53%	39%
6-10 17	16	18	18	14
11-15 7	4	9	9	4
16-20 3	1	5	3	10
20 or more 17	10	23	17	33

It is not surprising that most companies have been subject to a mere handful of check fraud attempts. Fraudsters often try to "attack" companies in order to identify those whose payments methods can be most easily breached. If they find that an attack attempt faces security "obstacles," fraudsters will move on. When fraudsters do succeed in their attacks, they likely will keep targeting an organization until security measures are put in place.

This last point may explain the relatively high percentage of companies that suffered from at least 20 fraud attempts in 2014. The good news is that the percentage of companies in that cohort decreased significantly from 27 percent in 2013 to 17 percent in 2014. This indicates that an increasing number of finance professionals are being proactive and their organizations have security measures in place to guard against fraud attacks.

Change in Check Fraud Attempts from 2013

(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)



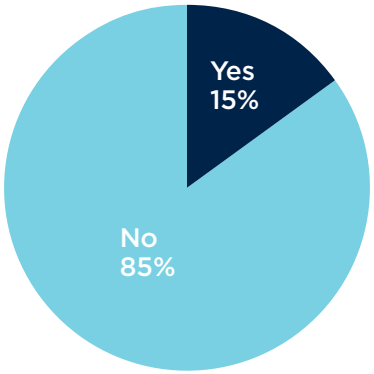
The method most often used by organizations to guard against check fraud is positive pay. This approach is used by 79 percent of organizations. Other popular methods of guarding against check fraud include "daily reconciliation and other internal processes" and "segregation of accounts." Larger companies—those with annual revenues of at least than $1 billion—are more likely than smaller ones to focus their efforts on positive pay (86 percent versus 72 percent).

Fraud Control Procedures Used to Guard Against Check Fraud
(Percent of Organizations that Suffered at Least One Attempt of Check Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Positive pay				
79%	72%	86%	88%	80%
Daily reconciliation and other internal processes				
73	69	75	74	76
Segregation of accounts				
66	67	65	66	62
Payee positive pay				
44	36	50	48	52
"Post no checks" restriction on depository accounts				
39	31	45	43	48
Reverse positive pay				
13	12	16	14	22
Non-bank fraud control services				
10	12	9	6	20

While check fraud was the most prevalent type of payments fraud experienced by organizations in 2014, the overwhelming majority of organizations did not suffer any financial loss as a result of such fraud. Only 15 percent of companies exposed to at least one check fraud attempt in 2014 incurred a financial loss as a consequence. The share rose to 28 percent among large companies with more than 100 payment accounts.

Suffered Financial Loss as a Result of Check Fraud
(Percentage Distribution of Organizations that Suffered from at Least One Attempt of Check Fraud)



Organizations incurred financial loss due to check fraud for various reasons:

- Account reconciliation or positive pay review not timely (cited by 34 percent of respondents)
- Internal fraud (24 percent)
- Gaps in online security control/criminal account takeover (15 percent)

Some survey respondents also report that clerical errors at their companies contributed to financial losses due to check fraud.

Finance professionals are keen to mitigate check fraud and are well aware that certain check features are effective in preventing such fraud. The two most effective features in preventing fraud are the use of controlled check stock which is not readily available to fraudsters (cited by 59 percent of survey respondents) and the use of dual-time true watermark (44 percent). Using more secure check stock can prevent the most common kinds of check fraud (e.g., altering either the MICR line, the amount or payee credentials). Using blank check stock also prevents bank information from being exposed.

Controlled check stock and the use of dual-time true watermark are most effective in preventing check fraud

Checks Features Most Effective in Preventing Fraud
(Percent of Respondents)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Controlled Check Stock (not readily available to fraudsters)				
59%	55%	60%	63%	55%
Dual-tone True Watermark				
44	43	45	46	49
Chemically reactive paper				
28	28	31	30	35
Thermochromatic (heat-sensitive) ink				
26	28	24	24	30
Toner Anchorage				
14	12	15	16	14
Other				
17	27	18	16	18

ACH Fraud

ACH transactions are more complex than check payments and therefore more challenging for criminals to hack. Successful ACH fraud attempts involve sophisticated techniques that are not readily available to many fraudsters. In order to commit fraud on ACH transactions, fraudsters need to access a customer's credentials, generate ACH files in the originator's name or build a fake customer profile. ACH hackers frequently have accomplices operating within organizations to assist with such fraud attempts.

In 2014, one-quarter of organizations were subject to ACH debit fraud and 10 percent to ACH credit fraud. Even among those organizations that have been subject to ACH fraud attempts, such fraud occurs infrequently. Seventy-three percent of organizations experienced one to five instances of ACH fraud in 2014. Only nine percent of survey respondents report their organizations experienced greater than 20 instances of ACH fraud. Larger companies with more than 100 payment accounts were three times more likely than similarly sized companies with fewer payments accounts to have been exposed to ACH fraud more than 20 times.

A vast majority of finance professionals (81 percent) report that the number of ACH fraud attempts at their companies in 2014 was unchanged from that reported in 2013. Only 13 percent report an increase in the instances of ACH fraud in the same timeframe. This is far less than the 36 percent who reported an *increase* in instances of ACH fraud in 2013 compared to 2012.

Attempted or Actual ACH Fraud in 2014

(Percentage Distribution of Organizations that Suffered at Least One Attempt of ACH Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
1-5 73%	79%	69%	78%	52%
6-10 10	10	10	9	15
11-15 5	4	6	4	7
16-20 4	2	5	3	7
More than 20 9	5	10	6	19

Eleven percent of organizations that were victims of at least one ACH fraud attempt in 2014 suffered a financial loss as a result. The share increases to 26 percent among larger companies with more than 100 payment accounts.

The most likely reasons why organizations were victims of ACH fraud include:

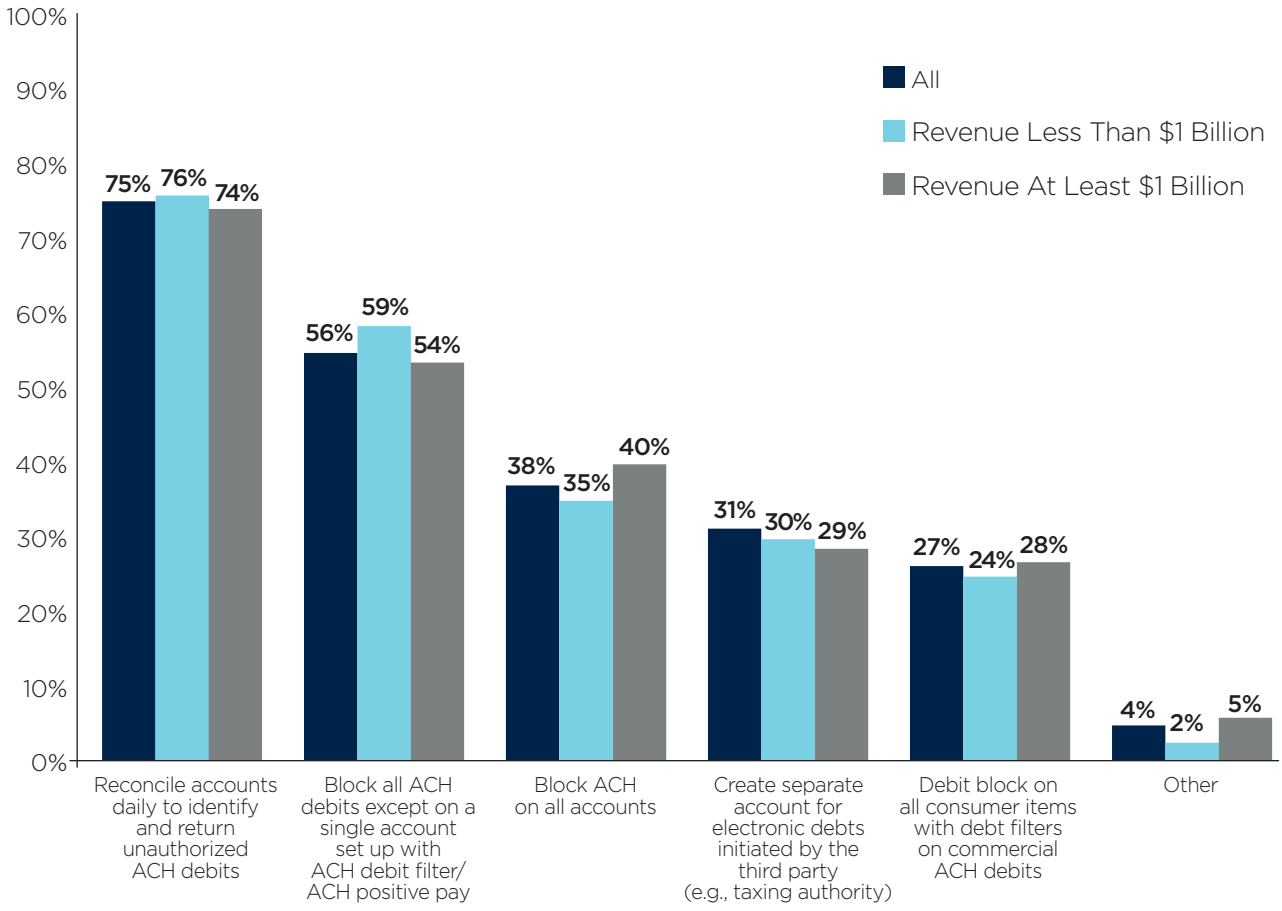
- ACH return not timely (cited by 40 percent of respondents)
- Did not use ACH debit blocks or ACH debit filters (40 percent)
- Did not use ACH positive pay (36 percent)
- Account reconciliation not timely (28 percent)
- Gaps in online security controls/criminal account takeover (24 percent)
- Internal fraud (16 percent)

Organizations can adopt various measures to protect against ACH fraud. Three-fourths of companies reconcile accounts daily to identify and retain unauthorized ACH debits while 56 percent block all ACH debits except those with ACH debit filter and/or ACH positive pay. Thirty-eight percent take the additional step of blocking ACH debits on all accounts.

Even the occasional occurrences of ACH fraud are evidence that some criminals are fairly sophisticated in their approach. They are usually well-prepared, often having done research on the target organization and may even be working with someone inside the company. Even though ACH fraud is not as common as check fraud, the actual breach may be deeper with more sensitive information being compromised.

Fraud Control Procedures Used to Prevent ACH Fraud

(Percent of Organizations that Suffered at Least One Attempt of ACH Fraud)



Corporate/Commercial Card Payments

Organizations increasingly use corporate/commercial cards for their business-to-business (B2B) payments. The most extensively used B2B cards in 2014 were purchasing cards (used by 71 percent of organizations), followed by travel & entertainment (T&E) cards (39 percent) and ghost or virtual cards (31 percent). A vast majority (97 percent) of finance professionals from larger organizations with more than 100 payment accounts indicate their companies use purchasing cards.

Corporate/Commercial Cards Used for B2B Payments

(Percent of Organizations)

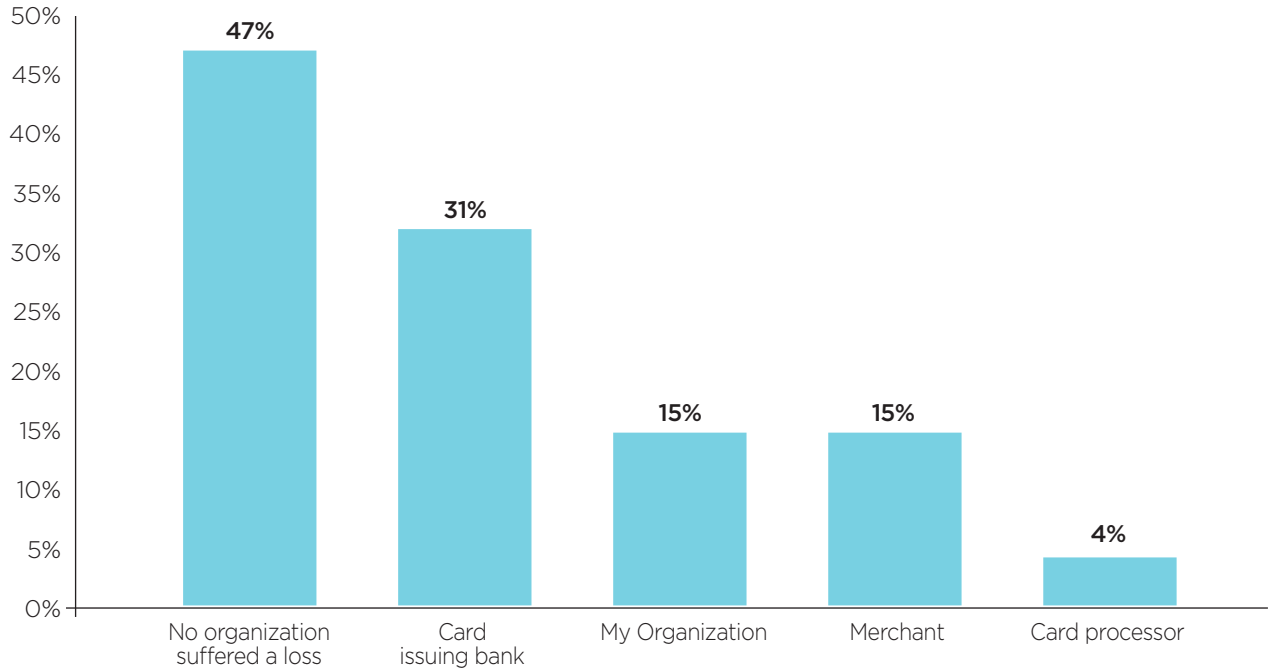
All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Purchasing cards				
71%	67%	76%	71%	97%
T&E cards				
39	36	42	44	39
Ghost or virtual cards (valid card account without a physical card issued)				
31	28	35	33	45
"One card" combining several uses above				
20	21	18	15	16
Fleet cards				
17	16	18	17	16
Airline travel cards (UATP)				
4	3	5	6	6
Other				
1	1	2	2	3

But as the use of such cards for B2B payments increases, so does the possibility of fraud via such vehicles. Indeed, corporate/commercial credit cards are the second most frequently targeted payment method for those attempting to commit payments fraud. Thirty-two percent of organizations that experienced fraud from cards in 2014 were impacted by fraud associated with their own commercial cards.

As occurs with other payment methods, corporate/commercial credit card fraud can result in a financial loss to companies as well as to other parties. While nearly half of organizations (47 percent) that were subject to such fraud in 2014 did not incur a loss due to the fraud, 15 percent did suffer a financial loss as a consequence. Other parties that suffered financial loss as a result of corporate/commercial fraud include the banks or financial institutions that issued the card (31 percent), the merchants (15 percent) and the card processors (4 percent).

Parties That Suffered Loss from Fraud on Corporate/Commercial Cards

(Percent of Organizations that Suffered at Least One Attempt of Corporate/Commercial Card Fraud)

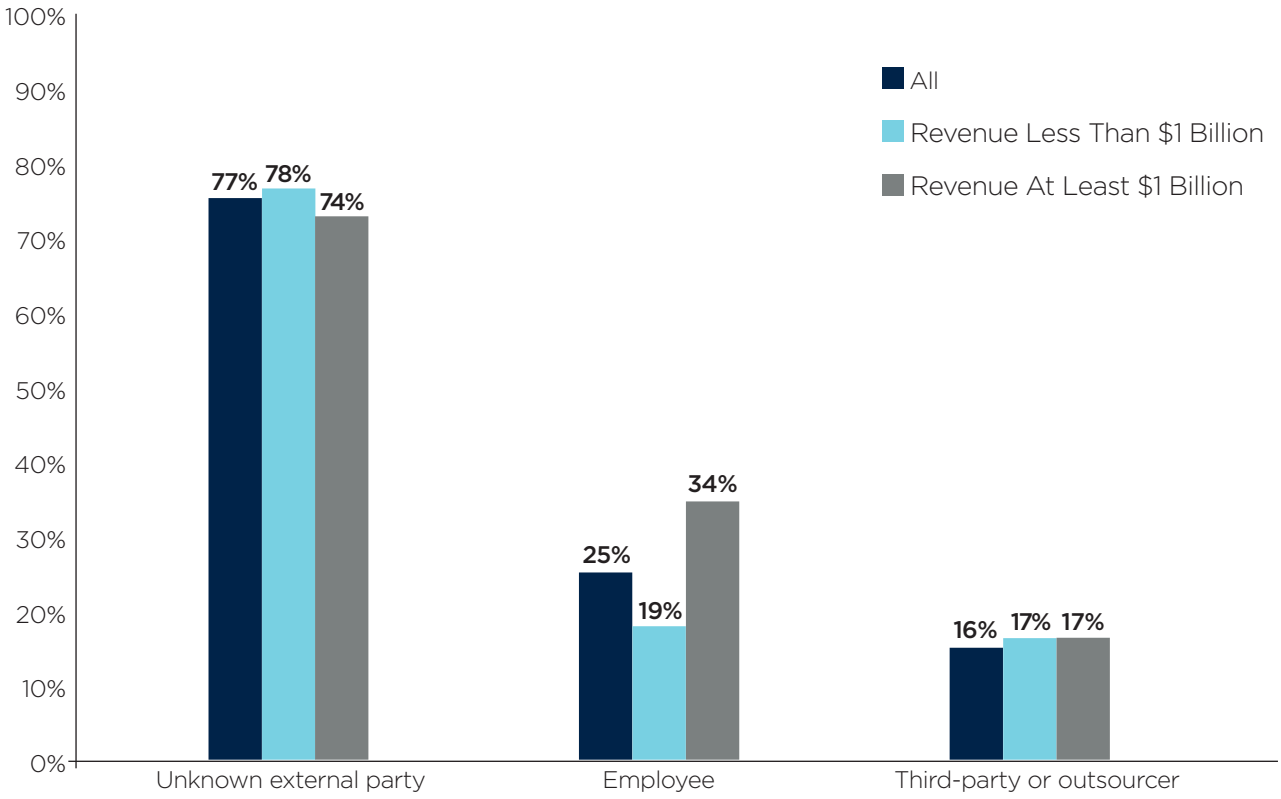


For 77 percent of organizations that were subject to fraud via their own corporate/commercial cards, the fraud was initiated by an unknown external party; for 16 percent of such companies, the fraud was committed by a known third-party such as a vendor or professional services provider. Interestingly, 25 percent of this type of fraud is perpetrated by a company's own employees, although this is less than the 40 percent reported in 2013. Larger companies with annual revenues of at least $1 billion are more likely than smaller ones (revenues less than $1 billion) to have been a victim of fraud initiated by one of their own employees (34 percent vs 19 percent).

Fraudulent card charges made by a third party are a primary cause for the financial losses that stem from the use of corporate/commercial cards (cited by 54 percent of financial professionals). Lack of internal controls (18 percent) and employee thefts (15 percent) also result in loss but were reported by fewer survey respondents.

Party Responsible for Fraud on Corporate/Commercial Cards

(Percent of Organizations that Suffered at Least One Attempt of Corporate/Commercial Card Fraud)



Mobile Payments

Mobile payments are a relatively new payment method. But in the view of finance professionals, consumers are chiefly concerned about the security of mobile payments and therefore are hesitant to wholly embrace it. Corporate practitioners from larger organizations (annual revenues of at least $1 billion) are more likely than those from smaller companies to cite this as a chief concern among their consumers (84 percent vs. 73 percent). Survey respondents suggest there are other security issues preventing greater use of mobile payments such as transmitting financial data over cell phone networks (54 percent) and potential exposure of personal financial information resulting from the loss of a phone (53 percent).

Mobile payments are fairly recent entrants into the payments field; this could explain the uncertainty surrounding the security of this payment method. Finance professionals themselves have numerous questions regarding mobile payments and the measures being used to safeguard those payments. There are also concerns about whether information is being transferred securely and if there is a risk of sensitive information being exposed. As mobile payments become equipped with security features such as tokenization and biometric authentication which do not impact their usability, they will be more widely accepted as a payment solution.

78% of financial professionals believe concerns about security are keeping consumers from embracing mobile payments

Security Issues Preventing Consumers from Further Embracing Mobile Payments
(Percent of Organizations)

	All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Concerns about whether mobile payments are a secure payment method	78%	73%	84%	83%	78%
Transmitting financial data over cell phone networks	54	52	56	55	62
Potential exposure of personal financial information resulting from a loss of the phone	53	49	56	57	55
The authentication process	26	22	28	27	26
Other	3	3	3	3	3

Credit/Debit Card Payments

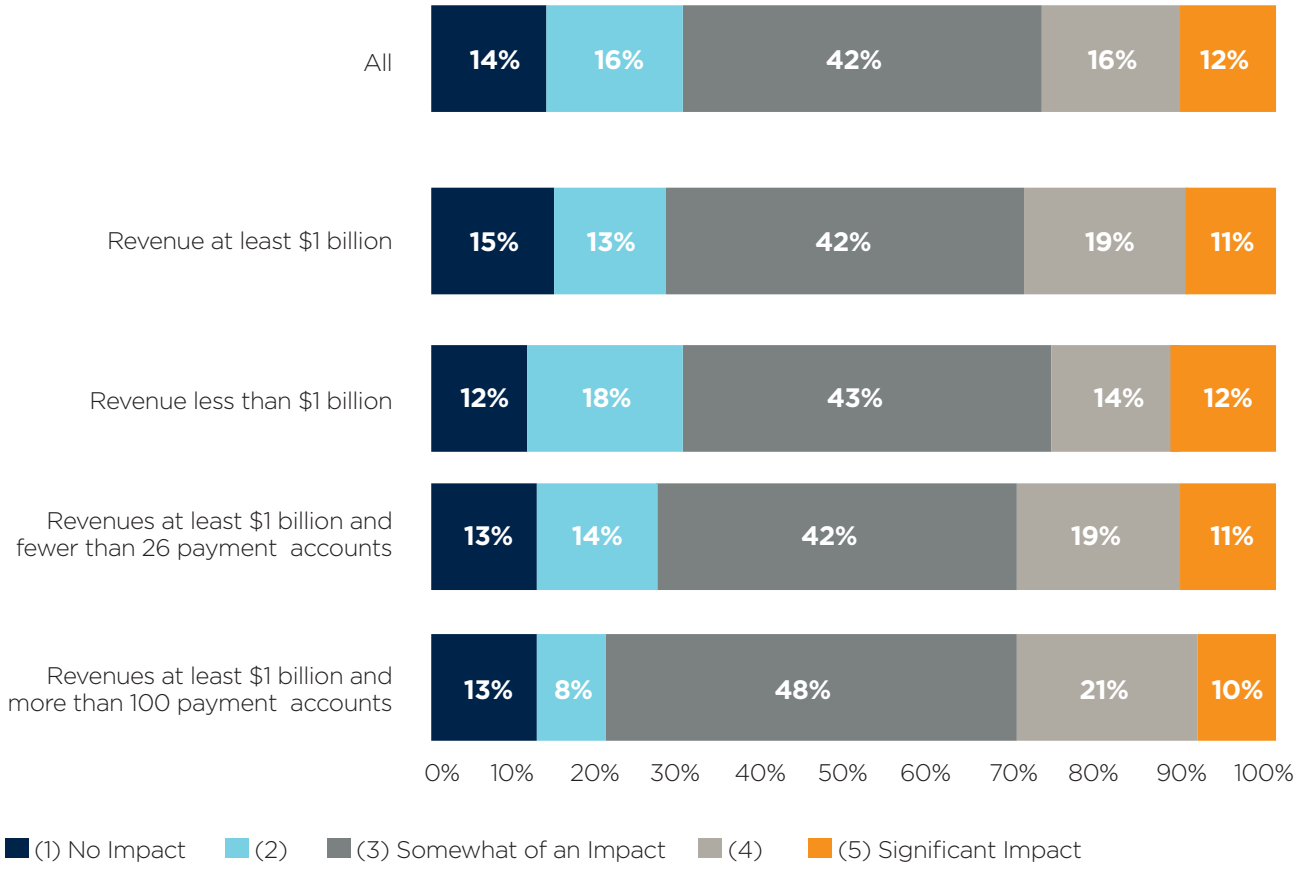
Seven out of ten finance professionals report that their organizations accept debit/credit card payments from customers. This result is consistent regardless of organization size or number of payment accounts maintained.

The elevated levels of credit/debit cards fraud first observed in last year's survey (33 percent versus 29 percent reported in *2013 AFP Payments Fraud Report*) has not abated. It continues to be of significant concern as 34 percent of organizations experienced such fraud in 2014. The issues that stem from this type of fraud are problematic for companies that rely on recurring payments from stored credit/debit cards and unsettling for those consumers whose personal data has been exposed. Additionally, credit-card issuers are forced to cancel and re-issue new cards, often with not much notice and faced with incurring unpaid charges since the stored information in the cards is now invalid.

The deadline for the upcoming shift in liability from card issuers to merchants is scheduled for October 2015. Twenty-eight percent of finance professionals foresee a significant impact from this on their organizations' investments in card fraud prevention methods/solutions while 42 percent anticipate a smaller impact.

Impact of Liability from Issuers to Merchants in Organization's Investment in Card Fraud Prevention Methods/Solutions

(Percentage Distribution of Organizations that Accept Credit/Debit Cards from Customers)



The use of EMV-chip cards is likely to have an impact on credit/debit card fraud. Smart chip technology dates back to the mid-1970s and the use of the smart chip in credit and debit cards began in the mid-1990s when the first version of the EMV (Europay, MasterCard, VISA) system was released. EMV cards have been used in many developed countries for the past decade, but the EMV system has not yet gained similar traction in the U.S. With the upcoming liability shift in October 2015, there appears to be a greater level of interest in the system. The chip card when used with a PIN code for authorizing transactions is considerably safer than using a card with a magnetic stripe and signature authorization. As chip cards continue to be introduced in the U.S., the authentication method will likely be a choice of either PIN or signature, so called Chip-and-Choice. However, if the Chip and PIN method is not widely adopted, consumers will be using the more secure chip cards while the authentication method may still be in the form of a lesser secure signature method.

When EMV-chip cards are more widely issued and used, fraudsters are likely to shift their focus to those payment methods which are less secure. Eighty percent of finance professionals believe that if EMV-chip cards are successful in reducing card acceptance fraud, fraudsters will shift their focus to other payment methods. This is a ten-percentage-point increase from the share of finance professionals holding the same view last year. Over a third (38 percent) anticipate that checks will be impacted the most, followed by ACH debit (24 percent) wire transfers (7 percent) and ACH credit (4 percent). The share of those who believe checks will be subject to greater fraud activity if EMV-chip cards are successful in mitigating fraud has declined considerably from 54 percent in 2013 to 38 percent in 2014.

EMV-chip card use will not prevent all fraud via cards just as the technology by itself does not prevent fraud on card-not-present (CNP) transactions such as online purchases. While there are security measures available for these transactions, at present they are not being used extensively in the U.S.

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Checks				
38%	41%	33%	40%	24%
ACH Debit				
24	20	29	30	22
Wire Transfers				
7	6	8	6	10
Other				
7	8	6	8	3
ACH Credit				
4	4	5	3	9
I don't believe fraud would migrate to other payment forms				
20	20	20	13	31

A vast majority of survey respondents (92 percent) firmly believe EMV cards will be effective in reducing point-of-sale (POS) fraud. Sixty-one percent of finance professionals believe that Chip-and-PIN will be the most effective authentication method in mitigating fraud. To authenticate a fraudulent Chip-and-PIN transaction, fraudsters will need both the stolen card/credentials and the card's associated PIN. The requirement of a PIN to carry out a transaction makes this method more effective in preventing any type of theft.

Other methods finance professionals feel will be successful in reducing POS fraud are EMV regardless of authentication method used (13 percent), Chip-and-Choice (12 percent) and Chip-and–Signature (7 percent). Finance professionals from larger companies (annual revenues at least $1 billion) are more likely than their peers at smaller organizations to believe that Chip-and-PIN will be successful.

92% of finance professionals firmly believe EMV cards will be effective in reducing point-of-sale fraud.

61% of finance professionals believe that Chip-and-PIN will be the most effective authentication method in mitigating credit/debit card payments fraud

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Chip-and-PIN				
61%	57%	64%	68%	60%
EMV will be effective in reducing POS card fraud regardless of authentication method used				
13	16	10	5	14
Chip-and-Choice (Merchant can chose PIN or Signature)				
12	13	12	16	9
Chip-and-Signature				
7	6	7	6	11
No authentication method will be effective in reducing POS card fraud				
8	9	7	5	7

Securing Credentials

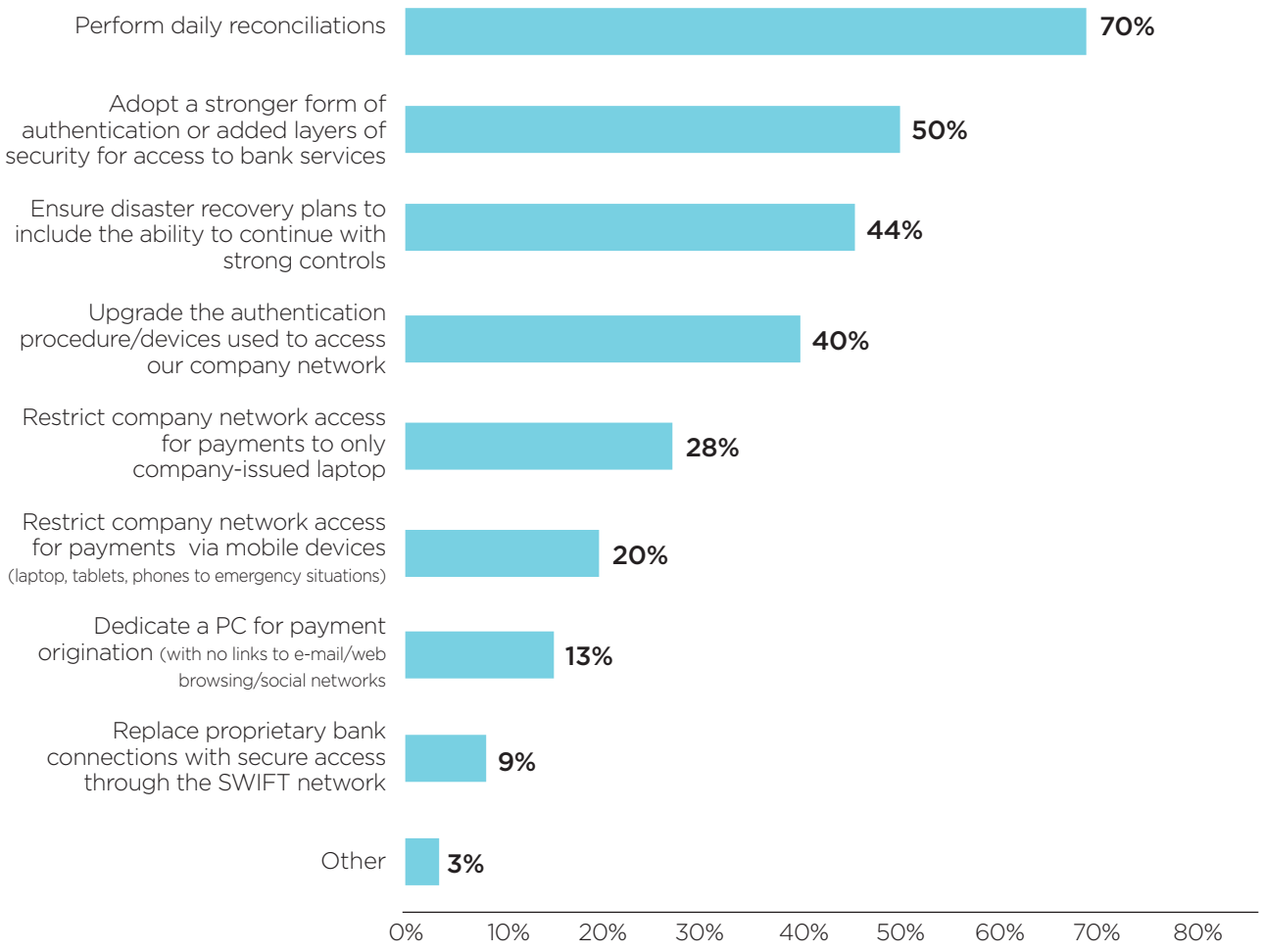
Widespread high-profile security breaches at major retailers in the U.S. are keeping major corporations on alert. These security breaches have had far-reaching consequences; consumers' personal data have been compromised and there has been reputational damage to the organizations that have been victims of these attacks. To guard against these breaches, companies are adopting various measures to protect themselves as well as their consumers.

- **Seven out of ten organizations** are conducting daily reconciliation of transaction activity. Reconciling also involves constant follow-up on questionable activity either internally or with the company's bank.
- **Half of organizations** are adopting a stronger form of authentication or added layers of security for access to bank services.
- **Forty-four percent of companies** are implementing systems to ensure that disaster recovery plans include the ability to continue with strong controls and maintain in-office compliance when enacting disaster recovery.
- **Two out of five organizations** are upgrading the authentication procedures/devices used to access their networks.

Other tactics organizations are adopting to guard against potential attacks include restricting company network access for payments to company-issued laptops only (28 percent) as well as restricting network access for payments via mobile devices (20 percent).

Daily reconciliation of transaction activity continues to be the practice financial professionals most often employ to guard against fraud. This process ensures fraudulent transactions are exposed with minimum delay and therefore can mitigate any damage resulting from the attack. Implementation of stronger authentication procedures is also popular as it adds more layers of security and makes it more difficult for fraudsters to penetrate. Fraudsters are unlikely to spend large amounts of time trying to expose highly protected information and would rather shift their focus to more vulnerable targets.

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



Conclusion

Data and payment breaches are increasingly more common and vital business, financial and personal data are being compromised. Malicious fraudsters are using more sophisticated techniques to circumvent various payment systems and target companies and their customers. Even when these criminals are unsuccessful in accessing direct funds, they often have been able to access confidential personal data, allowing them to steal identities of unsuspecting individuals and initiate other elaborate fraud attacks and breach even more secure payment methods.

Finance professionals realize how critical it is to keep their organizations' information secure and, as much as possible, prevent breaches of company payment systems. The costs of remediating the impact from payments fraud can be exorbitant and have long-term effects on those companies that fall victim to such malicious attacks.

Results from the *2015 AFP Payments Fraud and Control Survey* reveal key trends in the payments fraud area. Notable among these are the following:

The majority of companies continue to be impacted by payments fraud. Sixty-two percent of finance professionals report that their organizations were targets of payments fraud in 2014.

A vast majority of payments fraud originates from outside an organization. Three-fourths (76 percent) of organizations that experienced attempted or actual payments fraud in 2014 did so as a result of actions by an outside individual.

Checks continue to be the payment method most often targeted by those committing fraud attacks as well as the method accounting for the largest dollar amount of loss from such fraud. Seventy-seven percent of organizations that experienced attempted or actual payments fraud in 2014 were victims of check fraud.

Finance professionals are most concerned about whether mobile payments are a secure payment method. More than three-quarters of survey respondents believe that consumers are concerned about the secureness of mobile payments and therefore are hesitant to wholly embrace these types of payments.

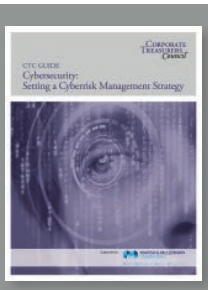
More than nine out of ten finance professionals believe that the use of EMV-chip cards will be effective in reducing point-of-sale fraud. A majority of finance professionals also indicate that Chip-and-PIN will be the most effective authentication method in mitigating fraud.

Preventing and defending against payments fraud is a challenge for companies. But they can limit their exposure and minimize losses due to such activity. Staying vigilant is an absolute necessity. Having adequate security measures in place will help reduce some if not most of the risk of and impact from payments fraud.

There are a number of effective tactics being used by finance professionals to reduce fraud risk.

- Positive pay and daily reconciliation to combat check fraud.
- Use of controlled check stock or blank check stock to limit the exposure of sensitive information
- Daily reconciliation of accounts to identify and return unauthorized ACH debits to prevent ACH fraud.
- Use of stronger forms of authentication with added levels of security to access bank services.

Finance professionals are fully aware of the uptick and severity of payments fraud breaches that occurred in 2014. They are on heightened alert. Being cognizant of the potential for attacks is a small but firm step in the fight against payments fraud.



Additional recommendations on mitigating cyberfraud available in the *CTC Guide to Cybersecurity*, which can be accessed at **www.ctc.AFPonline.org/guides/**

About the Survey

In January 2015, the Research Department of the Association for Financial Professionals® (AFP) surveyed 13,361 of its corporate practitioner members and prospects. The survey was sent to corporate practitioners members with the following job titles: cash manager, analyst and director. After eliminating surveys sent to invalid and/or blocked email addresses, the 433 responses yielded a response rate of 8 percent. Additional surveys were sent to non-member corporate practitioners holding similar job titles and generated an additional 308 responses for a total of 741 responses.

AFP thanks J.P. Morgan for underwriting the *2015 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.

Types of Organization's Payment Transactions

(Percentage Distribution)

	When Making Payments	When Receiving Payments
Primarily consumers	5%	21%
Split between consumers and businesses	22	29
Primarily businesses	72	50

Number of Payment Accounts Maintained

(Percentage Distribution of Organizations)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Fewer than 5 30%	41%	20%	37%	–
5-9 18	21	16	29	–
10-25 16	14	18	34	–
26-50 8	5	10	–	–
51-100 7	6	9	–	–
More than 100 20	14	26	–	100

Annual Revenues (USD)

(Percentage Distribution of Organizations)

Under $50 million	10%
$50-99.9 million	5
$100-249.9 million	11
$250-499.9 million	11
$500-999.9 million	14
$1-4.9 billion	27
$5-9.9 billion	9
$10-20 billion	7
Over $20 billion	7

Ownership Type

(Percentage Distribution of Organizations)

Publicly Owned	43%
Privately Held	36
Non-profit (not-for-profit)	12
Government (or government-owned entity)	9

Industry Classification

(Percentage Distribution of Organizations)

Banking/Financial services	11%
Business services/Consulting	4
Construction	2
Energy (including utilities)	9
Government	6
Health services	8
Hospitality/Travel	4
Insurance	7
Manufacturing	20
Non-profit (including education)	7
Real estate	4
Retail (including wholesale/distribution)	8
Software/Technology	5
Telecommunications/Media	3
Transportation	2

Appendix: Survey Data Tables

Payment Method Subject to Attempted or Actual Payments Fraud in 2014
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)

All (2014)	All (2013)	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Checks					
77%	82%	66%	82%	79%	86%
Credit/Debit Cards					
34	43	38	30	26	47
Wire transfers					
27	14	25	27	24	28
ACH debits					
25	25	20	30	28	37
ACH credits					
10	9	7	10	6	19

Change in Prevalence of Payments Fraud in 2014 Compared to 2013
(Percentage Distribution of Organizations Subject to Attempted or Actual Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Increased				
28%	32%	26%	22%	21%
About the same				
61	54	65	66	74
Decreased				
11	14	9	12	5

Payment Method Responsible for Largest Dollar Amount of Fraud Loss
(Percentage Distribution of Organizations that Suffered Financial Loss from Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Checks				
45%	45%	38%	32%	43%
Corporate credit cards (e.g., purchasing, Fleet)				
25	22	23	25	14
Wire transfers				
20	20	18	18	24
ACH debits				
7	4	10	11	10
Corporate debit cards				
2	2	2	4	–
ACH credits				
1	–	–	–	–

Sources of Attempted/Actual Payments Fraud in 2014
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Outside individual (e.g., check forged, stolen card)				
76%	70%	82%	81%	84%
Organized crime ring				
17	12	22	18	26
Third-party or outsourcer				
12	12	12	10	16
Account takeover				
11	12	10	10	14
Internal party				
6	5	6	4	9
Lost or stolen laptop				
1	2	1	–	–
Compromised mobile device				
1	1	2	2	–
Other				
9	13	6	4	12

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Perform daily reconciliations				
70%	68%	72%	76%	61%
Adopt a stronger form of authentication or added layers of security for access to bank services				
50	44	55	50	60
Ensure disaster recovery plans include the ability to continue with strong controls				
44	42	46	40	58
Upgrade the authentication procedure/devices used to access our company network				
40	36	44	39	56
Restrict company network access for payments to only company-issued laptop				
28	25	32	30	42
Restrict network access for payments via mobile devices (laptop, tablets, phones) to emergency situations only				
20	17	23	17	37
Dedicate a PC for payment origination (with no links to e-mail/web browsing/social networks)				
13	14	11	11	14
Replace proprietary bank connections with secure access through the SWIFT network				
9	11	8	1	21
Other				
3	4	3	1	5

CHECK FRAUD

Change in Check Fraud Attempts from 2013

(Percent of Organizations Subject to Attempted or Actual Payments Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Increased 19%	19%	21%	18%	12%
About the same 72	71	72	73	80
Decreased 9	10	8	9	8

Suffered Financial Loss as a Result of Check Fraud

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes 15%	16%	14%	9%	28%
No 85	84	86	91	72

Reasons for Financial Loss Due to Check Fraud

(Percent of Organizations that Suffered At least One Attempt of Check Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Account reconciliation not timely				
25%	22%	29%	18%	36%
Internal fraud (e.g., employee responsible)				
18	22	11	9	7
ACH return not timely				
14	15	14	–	21
Did not use ACH positive pay				
13	15	11	–	14
Gaps in online security controls/criminal account takeover				
11	4	18	27	14
Did not use ACH debit blocks or ACH debit filters				
2	–	4	–	7
Other				
34	30	39	45	36

ACH FRAUD

Trends in ACH Fraud Attempts as Compared to 2013

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Increased				
13%	7%	17%	19%	11%
About the same				
81	84	78	78	86
Decreased				
7	9	5	3	4

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes 11%	10%	12%	7%	26%
No 89	90	88	93	74

Reasons for Financial Loss from ACH Fraud
(Percent of Organizations that Suffered At least One Attempt of Check Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
ACH return not timely 40%	22%	50%	40%	43%
Did not use ACH debit blocks or ACH debit filters 40	33	44	20	43
Did not use ACH positive pay 36	33	38	–	43
Account reconciliation not timely 28	11	38	40	29
Gaps in online security controls/criminal account takeover 24	33	19	20	29
Internal fraud (e.g., employee responsible) 16	22	13	20	14
Other 8	–	13	20	14

Fraud Control Procedures Used to Prevent ACH Fraud

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Reconcile accounts daily to identify and return unauthorized ACH debits				
75%	76%	74%	78%	74%
Block all ACH debits except on a single account set up with ACH debit filter/ACH positive pay				
56	59	54	50	59
Block ACH debits on all accounts				
38	35	40	43	33
Create separate account for electronic debits initiated by the third party (e.g., taxing authority)				
31	30	29	26	33
Debit block on all consumer items with debit filter on commercial ACH debits				
27	24	28	22	41
Other				
4	2	5	4	7

CREDIT/DEBIT CARDS

Acceptance of Credit and/or Debit Card Payments from Customers

(Percentage Distribution of Organizations)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes				
71%	70%	73%	73%	74%
No				
29	30	27	27	26

Impact of Liability Shift from Card Issuers to Merchants in Organization's Investment in Card Acceptance Fraud Prevention Methods/Solutions
(Percentage Distribution of Organizations that Accept Credit/Debit Cards from Customers)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Significant Impact (5) 12%	12%	11%	11%	10%
(4) 16	14	19	19	21
Somewhat of an Impact (3) 42	43	42	42	48
(2) 16	18	13	14	8
No Impact (1) 14	12	15	13	13

CORPORATE/COMMERCIAL CARDS

Organization's Own Corporate/Commercial Cards Used to Commit or in Attempt to Commit Fraud
(Percentage Distribution of Organizations that Suffered At Least One Attempt of Corporate/Commercial Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Yes 32%	41%	24%	17%	38%
No 68	59	76	83	63

Corporate/Commercial Cards Used for B2B Payments
(Percent of Organizations Subject to Attempted or Actual Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Purchasing cards				
71%	67%	76%	71%	97%
T&E cards				
39	36	42	44	39
Ghost or virtual cards (valid card account without a physical card issued)				
31	28	35	33	45
"One card" combining several uses above				
20	21	18	15	16
Fleet cards				
17	16	18	17	16
Airline travel cards (UATP)				
4	3	5	6	6
Other				
1	1	2	2	3

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Organization suffered no financial loss				
47%	41%	52%	56%	48%
Card issuing bank				
31	35	28	23	39
My organization				
15	14	15	11	23
Merchant				
15	15	15	16	6
Card processor				
4	8	1	1	3
Other				
6	6	4	4	3

Reasons for Loss Associated with Corporate/Commercial Cards
(Percentage Distribution of Organizations that Suffered At Least One Attempt of Corporate/Commercial Card Fraud)

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Fraudulent card charges made by a third party				
54%	53%	57%	56%	57%
Lack of internal controls				
18	24	14	22	14
Employee theft				
15	18	14	–	29
No segregation of duties				
3	–	–	–	–
Other				
10	6	14	22	–

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

All	Revenue Less Than $1 Billion	Revenue At Least $1 Billion	Revenue At Least $1 Billion and Fewer Than 26 Payment Accounts	Revenue At Least $1 Billion and More Than 100 Payment Accounts
Unknown external party				
77%	78%	74%	67%	83%
Employee				
25	19	34	20	25
Third-party or outsourcer				
16	17	17	27	8

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. Study reports 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.

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

Put Cyberfraud on Lockdown

In 2014 alone, 62 percent of companies were impacted by payment fraud. But that doesn't have to happen to your company. Get proactive about cybersecurity, and visit our Fraud Resource Center to find out how to identify fraud and protect your business.

jpmorgan.com/cb/fraud-prevention

Commercial Banking Treasury Services

J.P.Morgan

Certified Treasury Professional®

Showcase your expertise.

- ☑ Improving collection and disbursement processes
- ☑ Managing cross-border funds movement
- ☑ Mitigating payment risk exposures
- ☑ Utilizing various types of payment systems and internet technologies
- ☑ Building cost-effective relationships with financial service providers

The Certified Treasury Professional® (CTP) credential signifies that you have DEMONSTRATED THE KNOWLEDGE AND SKILLS to perform successfully in today's complex financial environment.

Join more than 30,000 PROFESSIONALS around the world who have earned this prestigious certification.

Upcoming Testing Window
June 1, 2015 – July 31, 2015

Final Application Deadline
April 24, 2015

Become a CTP.
www.CTPcert.org