2010 AFP Payments Fraud and Control Survey

Report of Survey Results

Underwritten by

J.P.Morgan

2010 AFP Payments Fraud and Control Survey

Report of Survey Results

April 2010

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

Payments Fraud and Control Survey

Introduction

2009 was the year of the "Great Recession." Companies faced the pressures of economic turmoil, financial crises, waning consumer demand and pervasive liquidity constraints. These challenges, coupled with the continued growth of electronic payments, provided opportunities for payments fraud. While most organizations were subject to payments fraud attempts in 2009, slightly less than a third report that the number of incidents increased from the previous year.

Each year since 2005, the Association for Financial Professionals (AFP) has examined the nature and frequency of fraudulent attacks on business-to-business payments and the industry fraud-risk tools that organizations use to control payments fraud. Continuing that research, in January 2010 AFP conducted its annual Payments and Fraud Control Survey to capture the payments fraud experiences of organizations during 2009. Results of that survey are reflected in this, the *2010 AFP Payments Fraud and Control Survey* report.

The report shows that payments fraud remains rampant: a majority of organizations experienced attempted or actual payments fraud in 2009. The results also underscore the importance of organizations' continued use of fraud control measures to mitigate risk and reduce exposure to losses from emerging assaults to payments.

AFP thanks J.P. Morgan for underwriting the *2010 Payments Fraud and Control Survey.* Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of the AFP Research Department. Information on the survey methodology can be found at the end of this report.

Highlights of Survey Results

The key findings of the *2010 AFP Payments Fraud and Control Survey* include:

- Seventy-three percent of organizations experienced attempted or actual payments fraud in 2009.
  - Large organizations were more likely to have experienced payments fraud than were smaller ones. Eighty-one percent of organizations with annual revenues over $1 billion were victims of payments fraud in 2009 compared with 63 percent of organizations with annual revenues under $1 billion.
- Thirty percent of survey respondents report that incidents of fraud increased in 2009 compared to 2008.
- Nine out of ten organizations (90 percent) that experienced attempted or actual payments fraud in 2009 were victims of check fraud. The percentage of organizations affected by payments fraud via other payment methods were:
  - ACH debit (25 percent)
  - Consumer credit/debit cards (20 percent)
  - Corporate/commercial cards (17 percent)
  - ACH credits (seven percent)
  - Wire transfers (three percent)
- Seventy percent of organizations that were victims of actual and/or attempted payments fraud in 2009 experienced no financial loss from payments fraud.
- Among organizations that did suffer a financial loss resulting from payments fraud in 2009, the typical loss was $17,100.

Fraud Control

- Organizations turn to a number of fraud control services provided by their banks, including:
  - Positive pay/reverse positive pay (83 percent)
  - ACH debit blocks (77 percent)
  - ACH debit filters (58 percent)
  - Payee positive pay (52 percent)
- "Post no checks" restriction on depository accounts (37 percent)
- Organizations decide to opt out of particular fraud control services such as positive pay, debit blocks or Universal Payment Identification Code (UPIC) for a number of reasons: cost/benefit does not justify using a particular service (37 percent), the organization uses internal controls to reconcile and identify fraud (17 percent), or the organization does not issue enough checks/payments to justify use of a particular service (12 percent).
- Organizations develop and/or modify internal business processes to mitigate potential payments fraud risks. Among the processes considered important include:
  - Increase the use of electronic payments for business-to-consumer and business-to-business transactions (83 and 88 percent, respectively)
  - Restrict the use of online data communications (80 percent)

- Stop providing payment instructions by phone or fax (78 percent)
- Reduce the number of bank accounts (76 percent)

- Organizations also use separate accounts for different payment methods as a fraud control technique. For example,
  - Sixty-seven percent of organizations have separate accounts for disbursement and collections.
  - Fifty-six percent of organizations have separate bank accounts for checks and ACH payments.
  - Forty-six percent of organizations maintain separate accounts for different payment methods and types.

Check Fraud

- Checks remain the payment method most frequently targeted by criminals to commit payments fraud. Among the most widely used techniques to commit payments fraud were:
  - Counterfeit checks using the organization's MICR line data (72 percent)
  - Alteration of payee names on checks issued by the organization (58 percent)
  - Alteration of dollar amount on checks issued (35 percent)
- Seventeen percent of organizations that were victims of at least one attempt of check fraud during 2009 suffered a financial loss resulting from check fraud.

ACH Fraud

- Eleven percent of organizations that were victims of ACH fraud during 2009 suffered a financial loss as a result of such fraud.
- Organizations that suffered a financial loss as a result of ACH fraud generally did so because they did not follow best practices and/or neglected to execute their own business rules as expeditiously as they should have, including: ACH return not being timely, a criminal takeover of the organization's online system, or not using ACH positive pay.

Business-to-Business Card Payments Fraud

- Seventy-three percent of organizations that experienced payments fraud via the use of an organization's own corporate/commercial card report that an unknown external party committed the fraud.
- Sixteen percent of those organizations that experienced fraud via the use of an organization's own corporate/commercial card report that the fraud was committed by a third-party, such as a vendor, professional services provider or business trading partner.
- Forty-three percent of organizations subject to fraud via use of their organization's corporate/commercial cards during 2009 suffered actual financial losses resulting from the fraud.
- Just one out of six organizations that accepted corporate/commercial cards from its business-to-business partners suffered a financial loss resulting from fraud using such cards.

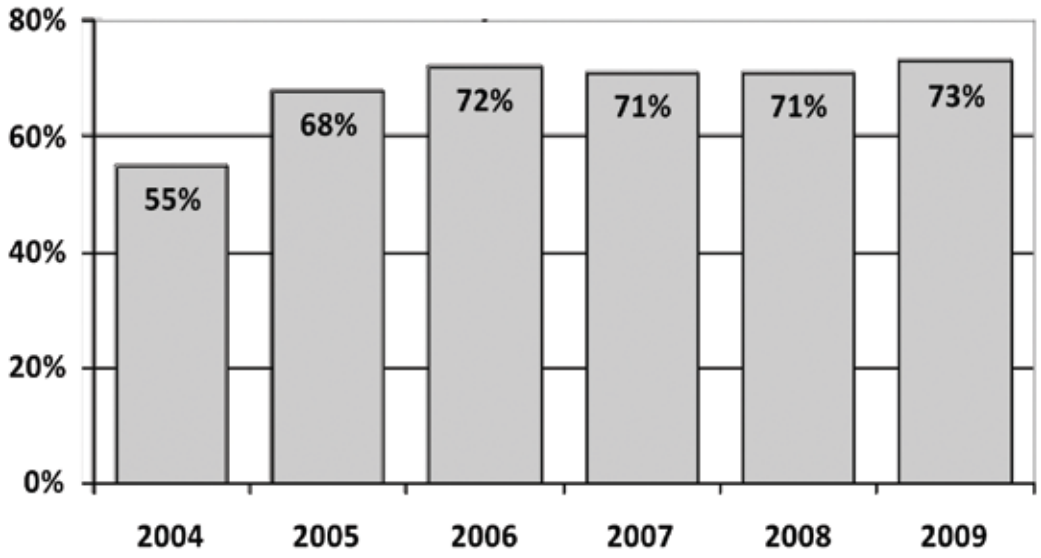
Survey Findings

Payments Fraud Overview

Most organizations were impacted by payments fraud during 2009. Fraud attacks on payment activities continued to occur at a greater frequency than that reported in the initial AFP payments fraud and control survey conducted in 2005 (reflecting 2004 data). The vulnerability of all payment methods—especially checks—to fraud from external and internal sources demand a range of fraud-fighting tools and the constant vigilance of financial and treasury professionals responsible for protecting the assets of their organizations.

Nearly three-quarters of organizations were victims of payments fraud in 2009. Seventy-three percent of organizations experienced attempted or actual payments fraud in 2009, the highest percentage of organizations reporting such fraud in the six-year history of the survey.

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



Large organizations were more likely to have been the targets of payments fraud than were smaller organizations. Eighty-one percent of organizations with annual revenues over $1 billion were victims of payments fraud in 2009 compared to 63 percent of organizations with annual revenues under $1 billion.

Organizations Subject to Attempted or Actual Payments Fraud in 2009
(Percent Distribution)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Organization was a victim of payments fraud	73%	81%	63%
Organization was not a victim of payments fraud	27	19	37

Nearly a third of organizations report that the number of payments fraud attempts increased in 2009 compared to 2008. Thirty percent of survey respondents indicate that incidents of payments fraud increased in 2009 from the previous year, while only 15 percent indicate that the number of incidents declined. The remaining 55 percent of respondents experienced no significant change in payments fraud activity from 2008 to 2009. The same percentage of organizations had reported increased fraud activity in the 2009 survey (based on 2008 data).

Change in Prevalence of Attempted Payments Fraud in 2009 Compared to 2008
(Percentage Distribution)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Increased incidents of fraud	30%	29%	31%
About the same	55	53	60
Decreased incidents of fraud	15	18	9

Even though their use continues to decline, checks remain the preferred target for criminals committing payments fraud. Nine out of ten organizations (90 percent) that experienced attempted or actual payments fraud in 2009 were victims of check fraud, just a single percentage point below that reported in the 2008 survey and four points below that in the 2007 survey. Following checks, the most popularly targeted payment types were:

- ACH debits (25 percent)
- Consumer credit/debit cards (20 percent)
- Corporate/commercial purchasing cards (17 percent).

Criminals appear to have taken a less "scattershot" approach to payments fraud in 2009, focusing instead on a few payment methods to commit such fraud, with each form of payment experiencing less fraud activity than had been reported in 2008.

Prevalence of Payments Fraud in 2009
(Percent of Respondents)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	90%	93%	89%
ACH debits	25	23	25
Consumer credit/debit cards	20	18	22
Corporate/commercial purchasing cards	17	18	13
ACH credits	7	5	4
Wire transfers	3	3	3

The growth in check fraud has far outpaced the growth in electronic payments fraud. Among organizations that experienced an increased incidence of payments fraud in 2009 compared to 2008, 89 percent indicate that check fraud increased over the past year. Just 13 percent report higher levels of consumer credit/debit card fraud and 11 percent report increased fraud involving ACH debits.

Large organizations—which are more likely to make/use electronic payments—are also more likely to have experienced an increase in payments fraud from ACH debits than were all organizations as a whole (15 percent versus 11 percent). Payments fraud from accepting consumer card payments was more likely to have occurred in small organizations than in large organizations (16 percent versus 11 percent).

Payment Methods Subject to More Payments Fraud in 2009 Compared to 2008
(Percent of Organizations Subject to Greater Amount of Attempted or Actual Payments Fraud in 2009)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	89%	85%	91%
Consumer credit/debit cards	13	11	16
ACH debits	11	15	3
Corporate/commercial purchasing cards	8	9	3
ACH credits	3	4	*
Wire transfers	2	2	3

Financial Loss from Fraud Attempts

While most organizations were subject to at least one payments fraud attempt in 2009, most of the fraud attempts involved relatively small amounts of money. For 47 percent of organizations that experienced payments fraud in 2009, the potential loss that could have resulted (or actually did result) from payments fraud was less than $25,000. For a third of organizations, the potential loss was between $25,000 and $249,000, while the potential loss was at least $250,000 for 19 percent of organizations.

The Potential Financial Loss Resulting from Attempted Payments Fraud in 2009
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Loss less than $25,000	47%	37%	60%
Loss between $25,000 and $49,000	9	9	9
Loss between $50,000 and $99,999	12	13	11
Loss between $100,000 and $249,999	13	16	7
Loss at least $250,000	19	25	13

Thanks to effective fraud detection tools and controls, the vast majority of organizations that were subject to at least one payments fraud attempt in 2009 did not suffer actual losses from the attempt. Seventy percent of organizations experienced no financial loss from payments fraud, while another 18 percent realized a financial loss of less than $25,000 during 2009. Among organizations that did suffer a financial loss resulting from payments fraud, the typical loss was $17,100. Larger organizations sustained a median loss of $19,000, 13.1 percent higher than the median loss sustained by smaller organizations.

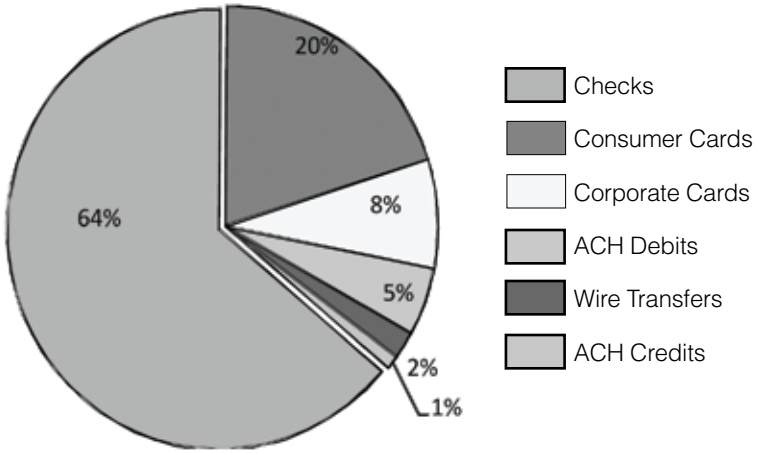
Actual Financial Losses from Attempted Payments Fraud in 2009
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
No loss	70%	73%	72%
Loss less than $25,000	18	12	20
Loss between $25,000 and $49,000	3	2	2
Loss between $50,000 and $99,999	5	6	6
Loss between $100,000 and $249,999	*	1	*
Loss at least $250,000	4	6	*
Median Loss#	$17,100	$19,000	$16,800

- Of organizations that sustained financial losses resulting from payments fraud in 2009.

Just as checks are the most likely target for payments fraud, they are also the payment type that results in the largest dollar amount of loss due to the actual fraud committed. Sixty-four percent of organizations that suffered financial loss resulting from payments fraud in 2009 suffered the greatest dollar loss from checks. The second most likely type of payments fraud resulting in the largest dollar loss is consumer credit/debit cards (20 percent), while the third largest source of dollar loss is corporate cards (e.g., purchasing, T&E, fleet).

Payment Method Responsible for the Greatest Financial Loss Resulting from Fraud in 2009
(Percentage Distribution of Organizations that Suffered Financial Loss from Payments Fraud)



For most organizations that were subject to attempted and/or actual payments fraud in 2009, the cost to manage, defend and/or clean up from payments fraud events was, at most, relatively modest. A third of organizations that were subject to at least one payments fraud attempt in 2009 did not expend any costs to defend against or clean up from the attempt. Fifty-five percent of organizations spent less than $25,000 in 2009.

Costs Spent to Manage, Defend and/or Clean Up Payments Fraud Events in 2009
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
No cost	35%	33%	37%
Less than $25,000	55	52	59
Between $25,000 and $49,000	4	5	2
Between $50,000 and $99,999	2	3	1
Between $100,000 and $249,999	2	3	1
At least $250,000	2	3	*

Most payments fraud is the result of an action taken by an individual who is not a part of the victimized organization. Eighty-seven percent of organizations that suffered a financial loss resulting from payments fraud in 2009 suffered the fraud from an outside individual (perhaps taking the form of forged check or a stolen credit/debit card). Fifteen percent of organizations were subject to payments fraud originating from an organized crime ring while 11 percent of organizations were subject to internal payments fraud.

Source of Payments Fraud that Resulted in Financial Loss in 2009
(Percent of Organizations that Suffered Financial Loss from Payments Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Outside individual (e.g., check forged, stolen card)	87%	87%	88%
Organized crime ring	15	15	12
Internal Party (i.e., malicious insider)	11	12	8
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	8	10	4
Criminal invasion (e.g., hacked system, malicious code-spyware or malware)	4	3	7
Other	4	2	6
Lost or stolen laptop or other device	2	1	2

Fraud Control

Organizations use a number of fraud control services offered by their financial institutions to protect their bank accounts. The most widely used fraud control measures used to guard against fraudulent checks are positive pay and/or reverse positive pay that compares a company's record of checks issued with checks presented for payment. Eighty-three percent of organizations use positive pay and/or reverse positive pay, including 85 percent of organizations with annual revenues greater than $1 billion. Just over half of all organizations (regardless of size) also protect against check fraud by using payee positive pay to circumvent the alteration of a payee name on checks. Thirty-seven percent of organizations place a "post no checks" restriction on depository accounts. Large organizations are more likely to use check-related fraud control measures than are smaller organizations.

Organizations continue to increase their use of controls that protect against ACH fraud. Seventy-seven percent of organizations use ACH debit blocks to prevent unauthorized ACH transactions while 58 percent use ACH debit filters for pre-authorized ACH debits from known trading

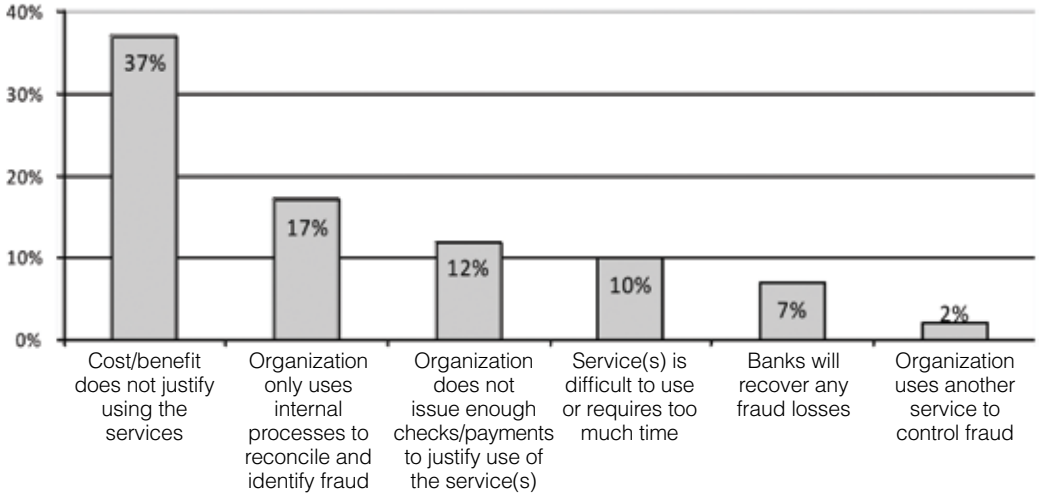
partners. (In the previous year's survey, 71 percent of organizations used ACH debit blocks and 55 percent used ACH debit filters.) The use of both of these ACH fraud control measures is greater among large organizations. Twenty-one percent of organizations use ACH positive pay while five percent use Universal Payment Identification Code (UPIC), which can be used to mask sensitive bank account information for ACH credits. In addition, two-thirds of organizations rely on internal processes (such as daily reconciliation) to prevent financial loss resulting from payments fraud. Eight percent also use non-bank fraud control services.

Services/Methods Used to Prevent Financial Loss from Fraud
(Percent of Organizations)

Payments	Types of Fraud Control Services	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	Positive pay/Reverse positive pay	83%	85%	81%
	Payee positive pay	52	60	45
	"Post no checks" restriction on depository accounts	37	46	26
ACH	ACH debit blocks	77%	83%	69%
	ACH debit filters	58	66	49
	ACH positive pay	21	18	20
	Universal Payment Identification Code (UPIC) for ACH credits	5	5	5
Other	Internal processes (e.g., daily reconciliation)	67%	69%	66%
	Non-bank fraud control services	8	8	6

While most organizations use positive pay and ACH debit blocks and/or filters to prevent payments fraud, they may decide not to use one of these services for a variety of reasons. The most widely cited reason is cost/benefit: 37 percent of organizations that do not use positive pay, debit blocks or UPIC choose not to do so because they do not believe the benefits outweigh the costs of using the service(s). Seventeen percent of organizations eschew these particular fraud control services because they choose to use internal processes to reconcile and identify fraud while 12 percent of organizations do not believe they issue enough checks to justify the use of these services.

Reasons for Not Using Positive Pay, Debit Blocks or UPIC
(Percent of Organizations Not Using Service)



In addition to purchasing fraud control services from their bank, many organizations develop their own internal measures and modify business processes to mitigate their risk of payments fraud. Eighty-eight percent of organizations that have increased their use of electronic payments for their business-to-business (B2B) transactions and 83 percent of organizations that have increased their use of electronic payments for business-to-consumer transactions did so with fraud prevention in mind. Four out of five organizations that have restricted their online data communications indicate that the desire to reduce payments fraud played an important role in the decision to do so. Seventy-eight percent of organizations report that fraud prevention was at least a "somewhat" important consideration when they decided to stop providing payment instructions by phone or fax.

Actions Taken as a Result of Controlling Fraud and Their Importance
(Percentage Distribution of Organizations Taking Particular Action)

	Important	Somewhat Important	Not at all Important
Increased use of electronic payments for B2C transactions (e.g., payroll cards, stored value cards, direct deposits to employee accounts)	51%	32%	17%
Increased use of electronic payments for B2B transactions	49	39	12
Stopped giving payment instructions by phone or fax	49	29	22
Restricted the use of online data communication	46	34	20
Reduced the number of bank accounts	43	33	24
Did not provide my bank account number to payors for electronic payments	38	32	30
Outsourced accounts payable	27	28	46

One best practice that organizations can follow is segregating accounts for different payment vehicles. Separation of accounts allows for more timely and focused review of payment activity.

Seventy-five percent of organizations maintain separate accounts for different payment methods and types. Two-thirds of organizations that maintain separate accounts have separate accounts for disbursement and collections, while 56 percent of organizations separate bank accounts for checks and ACH payments. Forty-six percent of organizations maintain separate accounts by payment type (e.g., vendor, tax, payroll, dividend).

Organizations' Maintenance of Separate Accounts for Different Payment Methods
(Percent of Organizations that Maintain Separate Accounts for Different Payment Methods or Types)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Separate accounts for disbursements and collections	67%	72%	60%
Separate accounts for checks and ACH payments	56	63	46
Separate accounts by payment type (e.g., vendor, tax, payroll, dividend)	46	42	49
Separate account for wire transfers	35	36	32
Separate account for card payments	24	25	23
Other	3	5	*

Check Fraud

The typical organization that was subject to attempted/actual check fraud in 2009 faced a median of six fraud attempts during the year. Forty-six percent of organizations were subject to between one and five check fraud events while 14 percent experienced between six and ten events. Twenty-seven percent of organizations saw a far greater number of check fraud events—more than 20. Large organizations were typically subject to twice as many check fraud events as were smaller organizations—eight versus four events.

Frequency of Attempted or Actual Check Fraud
(Percentage Distribution of Organizations Subject to At Least One Attempt at Check Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
1-5	46%	38%	61%
6-10	14	16	9
11-15	8	10	5
16-20	5	4	6
More than 20	27	32	19
Median # of incidents	6	8	4

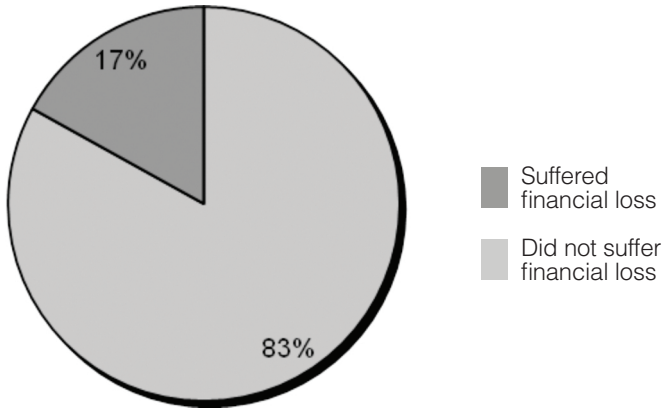
Seventy-two percent of organizations that were subject to check fraud in 2009 indicate that the fraud was perpetrated through the use of counterfeit checks using the organization's MICR line data. Fifty-eight percent of organizations that were subject to check fraud in 2009 report that the criminals altered payee names on checks issued by the organization, while 35 percent of organizations subject to check fraud report that the fraud resulted from alteration of the dollar amount on checks they had issued.

Types of Fraud Resulting from Using Checks
(Percent of Organizations that Suffered Check Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Counterfeit checks (other than payroll) with your organizations MICR line data	72%	77%	65%
Payee name alteration on checks issued	58	61	55
Dollar amount alteration on checks issued	35	36	32
Loss, theft or counterfeit of employee pay checks	21	22	17
Other	6	8	5

Even if check fraud is the prevalent type of payments fraud experienced by organizations, most of them do not suffer financial losses as a result. Seventeen percent of organizations that were subject to check fraud in 2009 report that they suffered financial loss from the check fraud. There was little difference in the likelihood that an organization suffered from check fraud by organizational size.

Check Fraud Resulting in Financial Loss
(Percentage Distribution of Organizations that Suffered Check Fraud)



Organizations that did suffer a financial loss resulting from check fraud identify a number of factors that led to the loss. Thirty-seven percent of organizations indicate that the check used in the fraud was cashed by a check-cashing service. Twenty percent of organizations did not use positive pay or reverse positive pay. Twenty percent of organizations did not reconcile their accounts on a timely basis, while 18 percent did not return checks on a timely basis. Sixteen percent of survey respondents indicate that the event involved internal fraud perpetrated by an employee of their organizations.

Cause of Loss due to Check Fraud
(Percent of Organizations that Suffered a Loss Resulting from Check Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Loss due to check cashed by check-cashing service	37%	46%	18%
Loss due to account reconciliation or positive pay review not being timely	20	25	12
Loss due to not using positive pay, reverse positive pay or payee positive pay	20	21	24
Loss due to untimely check return	18	18	18
Loss due to internal fraud (e.g., employee responsible)	16	18	12
Loss due to not using "post no checks" service on electronic payment account	10	11	12
Other (please specify)	25	29	24

A relatively small percentage of organizations experienced duplicate debits posted to their bank accounts as a result of a check having been deposited twice. Eighteen percent of survey respondents indicate that their organizations were subject to duplicate debits, with equal proportions of large and smaller organizations reporting such activity at similar rates.

Problems with Duplicate Debits Resulting from Same Check Deposit
(Percentage Distribution)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Organization did not have duplicate debits posted to an account because checks were deposited twice	82%	82%	84%
Organization had duplicate debits posted to an account because checks were deposited twice	18	18	16

In 71 percent of the cases, the duplicate debits were the result of operation error, with fraud being the cause in one out of five cases.

Reasons for Duplicate Debits Resulting from Same Check Deposit
(Percent of Organizations that Had Duplicate Debits Resulting from Same Check Deposit)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Operational Error	71%	70%	81%
Fraud	20	13	31
Don't know	29	40	6

With the passage of Check 21 legislation in 2003—which created a new negotiable instrument or the substitute check—the adoption of remote deposit capture has surged in recent years. Remote deposit capture services allow for scanned checks to be deposited electronically from the back office of a company to its bank account. Fifty-nine percent of survey respondents indicate that their organizations transmit check images using remote deposit – an increase of 15 percentage points since 2007.

Despite the increase in the use of remote deposit, there have been very few incidents of fraud originating from the use of the scanned checks. Just three percent of survey respondents whose organizations use remote deposit indicate their organizations were subject to payments fraud originating from the service.

Fraud As a Result of Remote Deposit Service
(Percentage Distribution of Organizations that Use Remote Deposit)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Check conversion service was not used as vehicle for fraud	97%	99%	95%
Check conversion service was used as vehicle for fraud	3	1	5

ACH Fraud

Not only does ACH fraud affect a relatively small number of organizations, it occurs rather infrequently even among those organizations that have been affected by it. Among organizations that were victims of attempted and/or actual ACH fraud in 2009, the typical organization was subject to three ACH fraud attempts during the year.

Frequency of Attempted or Actual ACH Fraud
(Percentage Distribution that Suffered ACH Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
1-5	68%	61%	75%
6-10	10	8	11
11-15	8	13	*
16-20	3	5	*
More than 20	12	13	14
Median # of incidents	3	4	3

Even though approximately three out of ten organizations were victims of at least one attempt of ACH fraud during 2009, barely more than one out of ten organizations suffered a financial loss as a result. Eleven percent of organizations that were victims of ACH fraud during 2009 also suffered a financial loss. Smaller organizations were likely to have suffered a financial loss from ACH fraud—18 percent—compared to nine percent of organizations with annual revenues greater than $1 billion.

There are a number of reasons why an organization would have been financially responsible for the losses sustained from ACH fraud. Among the most widely cited reasons are:

- ACH return not being timely
- A criminal takeover of the organization's online system was used to initiate the fraudulent transactions
- Organization did not use ACH positive pay
- Account reconciliation was not timely
- Organization did not use ACH debit blocks or ACH debit filters
- Inaccurate key entry (or error).

ACH Fraud Resulting in Financial Loss
(Percentage Distribution of Organizations that Suffered ACH Fraud)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Did not result in financial loss	89%	91%	82%
Resulted in financial loss	11	9	18

One out of six respondents from organizations that suffered ACH payments fraud in 2009 indicate their organizations received an ACH debit (ARC, POP, BOC, etc.) to their account that had the same check number as a previously received check transaction.

Fraudulent ACH Debits Resulting from a Fraudulent Check Transaction
(Percentage Distribution of Organizations that Suffered ACH Fraud)

Check did not have same check number as previously received check	51%
Check had same check number as previouslly received check	16
Do not know	33

Most organizations do not have difficulty in meeting the 24-hour deadline for returning ACH debits. Fifty-six percent of organizations that were subject to ACH fraud in 2009 indicate that they do not have any difficulty in meeting the 24-hour deadline for returning ACH debits. Thirteen percent of organizations "rarely" have difficulty in meeting the deadline while a quarter indicate that they "sometimes" have difficulty.

Organizations' Experience in Meeting 24-Hour Deadline for Returning ACH Debits
(Percentage Distribution)

Organizations does not have difficulty meeting the deadline	56%
Organization rarely has difficulty meeting the deadline	13
Organization sometimes has difficulty meeting the deadline	25
Organization regularly has difficulty meeting the deadline	6

There are a variety of actions that an organization can take in order to meet the 24-hour deadline for returning ACH debits. Forty-four percent of organizations return ACH debits if they cannot easily identify the originator of the debit. A quarter of organizations have identified the best practices that their peers use to manage the process while 14 percent provide a customer service number from the originator.

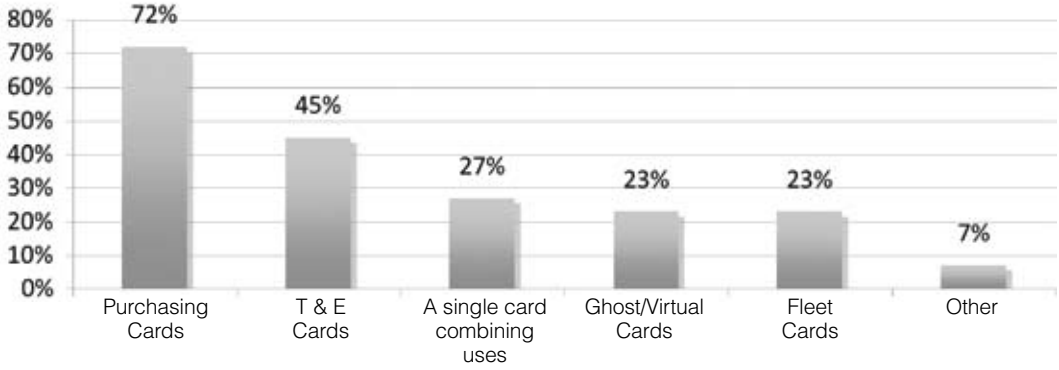
Actions to Aid Meeting 24-Hour Deadline for Returning ACH Debits
(Percentage Distribution)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Not a problem—organization returns ACH debits if the originator cannot be readily identified	44%	37%	53%
Identify best practices companies use to manage this process	24	27	23
Provide a customer service number from the originator	14	18	12
Ensure the company name is readily recognized	11	8	8
Other (please specify)	7	10	4

Business-to-Business Card Payments Fraud: Making B2B Card Payments

Seventy-seven percent of respondents indicate that their organizations use corporate/commercial cards for business-to-business (B2B) payments. Purchasing cards are the most likely used forms of corporate/commercial cards (72 percent), followed by travel and entertainment (T&E) cards (45 percent), cards that combine many uses (27 percent) and ghost or virtual cards (23 percent).

Types of Cards Used in Making B2B Payments
(Percent of Organizations that Suffered B2B Card Fraud)



Slightly more than two out of five organizations report that they experienced fraud in 2009 through the use of their own corporate/commercial cards.

Fraud Resulting from Organizations' Own Corporate/Commercial Cards
(Percentage Distribution of Organizations that Experienced Fraud Associated with Corporate/Commercial Cards)

	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Experienced Fraud	42%	48%	31%
Did not Experience Fraud	58	52	69

Typically, payments fraud involving an organization's own corporate/commercial cards is committed by an outside party. Nearly three-quarters of organizations that were subject to fraud committed using their own corporate/commercial card indicate that the fraud was perpetrated by an unknown external party (73 percent). Sixteen percent of such organizations report that the fraud was committed by a known third-party, such as a vendor, professional services provider or business trading partner. Despite the prevalence of corporate/commercial card fraud by outside parties, a significant amount of such fraud is committed by an organization's own employees. Just over a quarter of organizations were subject to fraud by their own employees using the organizations' corporate/commercial cards (27 percent).

Primary Party Responsible for Fraud from Making B2B Card Payments
(Percentage of Organizations that Suffered Attempted or Actual Fraud Using Organizations' Corporate/Commercial Cards)

External	Unknown external party	73%
	Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	16
Internal	Employee	27
Other	Other	*

When an organization's own checks were used to perpetrate payments fraud, those incidents frequently did not result in financial liability to the organization. But this is not typically true in cases of payments fraud involving corporate/commercial cards. Forty-three percent of organizations that were subject to corporate/commercial card fraud during 2009 suffered actual financial losses. Other parties that suffered financial loss as a result of corporate/commercial card fraud include the bank or financial institution that issued the card (49 percent) and the merchant where the card was used (27 percent).

When an organization is responsible for the financial loss associated with fraudulent use of its corporate/commercial cards, it is usually because of employee-caused loss (e.g., fraud).

Organizations Suffering Loss as a Result of B2B Corporate/Commercial Card Fraud
(Percent of Organizations that Suffered Attempted or Actual Fraud Using Organizations' Corporate/Commercial Cards)

Card issuing bank	49%
The organization	43
Merchant	27
No organization suffered financial loss	19
Other	11
Card processor	*

Business-to-Business Card Payments Fraud: Accepting B2B Card Payments

Just one out of six organizations that accept corporate/commercial cards from their business-to-business partners suffered a financial loss resulting from fraudulent use of such cards.

Financial Loss Due to Accepting Corporate/Commercial Cards in 2009
(Percentage Distribution of Organizations that Experienced Fraud Associated with Accepting Corporate/Commercial Cards)

Experienced financial loss	16%
Did not Experience financial loss	84

When an organization suffers a financial loss resulting from accepting a fraudulent B2B card payment, it is often because the organization failed to follow processes that would likely have prevented the fraudulent activity. Two-thirds of organizations that suffered a financial loss from accepting a fraudulent B2B card payment did so because the "card was not present" for the transaction (e.g., the card was accepted over the phone or via the Internet). Other reasons why organizations suffered a financial loss from a fraudulent card transaction include:

- Failure to authenticate the cardholder (44 percent)
- Failure to respond to a charge-back response in a timely manner (33 percent).

Primary Reason the Organization Suffered Losses from Accepting B2B Card Payments
(Percent of Organizations that Suffered a Financial Loss Resulting from Accepting B2BCard Payments)

Card-not-present merchant assumes liability	67%
Did not authenticate cardholder (e.g., cardholder's address)	44
Accepted fraudulent cards	44
Delayed charge back response	33
Other	33

Conclusions

With nearly three out of four organizations having been victims of fraud attempts or losses in 2009, it is clear that the payments fraud business is alive and well. Larger organizations continue to be favorite targets of the criminal element, as payments fraud was reported by 81 percent of organizations with revenues over $1 billion and 63 percent of those with revenues under $1 billion. However, criminals appear to have taken a less "scattershot" approach to fraud in 2009, focusing on fewer payment methods to commit fraud.

This development may have been driven by improved fraud control performance by organizations and their banks. Of those organizations that were targeted for fraud, the percentage that actually experienced financial losses from fraud declined from 37 percent in 2008 to 30 percent in 2009. Unfortunately, when fraudsters were successful, organizations paid a higher price. The typical financial loss from fraud increased by nearly 13 percent—from $15,200 in 2008 to $17,100 in 2009.

Large organizations face much higher exposures to fraud losses—54 percent of the potential fraud losses are over $50,000, while 60 percent of potential fraud losses are less than $25,000 for smaller organizations. Both large and small organizations experience losses at about the same rate, but the actual amount lost is 13 percent higher, on average, at larger organizations—with six percent of large organizations reporting actual losses exceeding $250,000. In addition, the costs incurred by large organizations to manage, defend, or clean up payments fraud is modestly higher than in smaller organizations, most likely due to the higher stakes those larger organizations have in trying to avoid losses.

By a wide margin, the favorite mechanism for criminals to commit fraud is checks. Indeed, despite the overall decline in the volume of checks issued, checks continue to be the largest source of payments fraud attempts against organizations. Of those organizations targeted for fraud, 90 percent of them experienced check fraud and 64 percent report that the greatest financial losses resulted from check fraud cases. In comparison, the next most popular payment method used to commit fraud was ACH debits—through which 25 percent of organizations were targeted. Overall, check fraud attempts at larger organizations are double the rate of that at smaller organizations. Incredibly, nearly a third of large organizations are forced to respond to new check fraud attempts every couple of weeks.

Fraudsters clearly have two favorite methods they use to target organizations of all sizes—counterfeit checks and altering the payee name on issued checks, experienced by 72 percent and 58 percent of organizations, respectively. The dollar amount is also altered on occasion, but only about a third of organizations report this problem. Depositing and clearing check images does not currently appear to be impacting fraud levels or loss rates.

Check fraud attempts are almost routine and most organizations manage to avoid actual losses. But organizations that actually did lose money due to payments fraud suffered the financial loss because they did not implement or follow routine or best practices. The

majority of the losses were due to a failure to use some type of positive pay or "post no checks" service, failure to perform a timely review of positive pay or account reconciliation, or not returning a check in the legally mandated time frame. The two main exceptions are payments fraud due to internal (employee) fraud or when checks are cashed at a check-cashing service, and when there is a holder in due course situation (duplicate check or stop payment issued on a check that was cashed). Except for positive pay/reverse positive pay, smaller organizations use bank fraud control services much less often than do their larger counterparts. Organizations that eschew fraud control services do so primarily because of the cost/benefit equation or lower transaction volumes, which make some sense given the lower average level of potential losses they face.

The criminal element has been less successful in using ACH to commit payments fraud. ACH volume continues to increase, but payments fraud levels via ACH are declining or leveling off. Part of this lack of success in ACH payments fraud is the limited ability of criminals to access the ACH network as well as widespread availability of fraud control tools at banks. Nearly 80 percent of organizations have fewer than ten ACH fraud attempts per year (no organization reported more than 20 incidents in a year) and only about one in ten experienced a financial loss. Debit blocks and filters are used by a clear majority of organizations and about a fifth of organizations use ACH positive pay. Somewhat surprisingly, use of the Universal Payment Identification Code (UPIC), which screens bank account information and is limited to ACH credits, continues to lag.

One issue of pressing concern is the ability of organizations to meet the 24-hour deadline for returning unauthorized ACH debits. There was some interest expressed among survey respondents increasing the amount of allowable time to 48 hours. However, increasing this return time creates the potential for unintended consequences, chief of which is the increased systemic risk to the parties that would be receiving returns later than they currently experience. In light of this, as well as taking into account the survey results indicating that 69 percent of organizations already deal with this deadline effectively, the AFP is working with NACHA to develop a statement of best practices to provide effective guidance to organizations.

In addition to using the payments fraud control measures mentioned earlier, most organizations also use internal account-level controls. These measures include daily account reconciliation, maintaining separate accounts for different applications (e.g., payroll vs. payables), payment types (e.g., ACH vs. checks), and purposes (e.g., disbursements vs. receivables). With account-level controls an important part of managing fraud, organizations are generating a greater need for tools to monitor and manage their bank accounts, including authorized signers. In the future, services such as Electronic Bank Account Management (eBAM) are likely to take on greater importance managing fraud losses and the cost of account opening and maintenance.

Payments fraud rates from the use of corporate/commercial cards are certainly not high compared to payments fraud committed via checks. However, when cards are used for fraudulent purposes—in both buying and selling situations—organizations tend to experience higher actual loss rates. When an organization allows employees to use company cards for purchases and fraud occurs, the organization was responsible for the financial loss 43 percent of the time. When the organization was a merchant accepting cards, the loss rate was as high as 67 percent for cards not presented at the time of transaction.

The survey results suggest that perhaps the single best way for organizations to protect themselves against payments fraud is to move away as quickly as possible from the use of checks for payment. While ACH and card fraud is not insignificant, the data in this and prior surveys makes it abundantly clear that issuing checks represents the greatest vulnerability to payments fraud for organizations. With the Federal Reserve consolidating check operations to one site, making all checks local, and check image clearing used for nearly all checks, check float is becoming a thing of the past and so should not be a reason for organizations to continue to issue checks. Organizations large and small should be pushing hard and working with their banks, vendors and other suppliers, to eliminate this vulnerability by moving transactions to ACH and card payments.

About the Respondents

In January 2010, the Research Department of the Association for Financial Professionals (AFP) surveyed 4,800 of its corporate practitioner members about payments fraud and controls. The survey was sent to AFP corporate practitioner members with the following job titles: cash managers, analysts, and directors. After eliminating surveys sent to invalid and/or blocked email addresses, the 416 responses yield an adjusted response rate of ten percent. Additional surveys were sent to non-member corporate practitioners holding similar job titles and generated an additional 69 responses. The following tables provide a profile of the survey respondents.

AFP thanks J.P. Morgan for underwriting the *2010 Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of the AFP Research Department.

The following tables provide a profile of the survey respondents.

Annual Revenues
(Percentage Distribution)

Under $50 million	5%
$50-99.9 million	3
$100-249.9 million	9
$250-499.9 million	11
$500-999.9 million	16
$1-4.9 billion	35
$5-9.9 billion	8
$10-20 billion	5
Over $20 billion	8

Industry Classification
(Percentage Distribution)

Manufacturing	20%
Retail (including wholesale/distribution)	12
Energy (including utilities)	11
Health services	10
Government	8
Insurance	8
Banking/Financial services	7
Non-profit (including education)	5
Real estate	4
Telecommunications/Media	4
Software/Technology	3
Business services/Consulting	2
Construction	2
Hospitality/Travel	2
Transportation	2

Ownership Type
(Percentage Distribution)

Publicly owned	44%
Privately held	35
Non-profit (non-for-profit)	13
Government (or government-owned entity)	8

Payment Methods Used to Make Payments in 2009
(Percent of Organizations)

Payment Methods	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	98%	97%	99%
Wire transfers	96	97	94
ACH credits	80	86	72
Corporate/commercial purchasing cards	77	82	70
ACH debits	75	76	75
Consumer credit/debit cards	23	21	26

Payment Methods Used to Accept Payments 2009
(Percent of Organizations)

Payment Methods	All Respondents	Revenues over $1 billion	Revenues under $1 billion
Checks	94%	94%	95%
Wire transfers	89	93	84
ACH credits	87	91	82
ACH debits	55	54	49
Consumer credit/debit cards	52	52	54
Corporate/commercial purchasing cards	39	41	35

Organization's Volume of Payments Transactions
(Percent Distribution)

Payment Methods	Primarily Consumers	Split Between Consumers and Business	Primarily Businesses
Making Payments	3%	22%	75%
Receiving Payments	22	29	49

AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. The AFP Research team is led by Managing Director, Research, Kevin A. Roth, PhD, who is joined by four research analysts. AFP Research also 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.

Association for Financial Professionals®

About the Association for Financial Professionals

The Association for Financial Professionals (AFP) headquartered in Bethesda, Maryland, supports more than 16,000 individual members from a wide range of industries throughout all stages of their careers in various aspects of treasury and financial management. AFP is the preferred resource for financial professionals for continuing education, financial tools and publications, career development, certifications, research, representation to legislators and regulators, and the development of industry standards.

General Inquiries AFP@AFPonline.org

Web Site www.AFPonline.org

Phone 301.907.2862