



# 2009 AFP Payments Fraud and Control Survey Report of Survey Results

Underwritten by  
**J.P.Morgan**

2009 AFP  
Payments Fraud  
and Control Survey  
Report of Survey Results

*March 2009*

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](http://www.AFPonline.org)

# Payments Fraud and Control Survey

## Introduction

2008 was a year of economic turmoil and financial crises that resulted in a housing collapse, mounting foreclosures, and pervasive liquidity constraints. Deteriorating financial conditions – especially in the second half of the year – coupled with the emergence of new payments types and the growth of electronic payments, also opened up new opportunities for payment fraud.

Since 2005, the Association for Financial Professionals (AFP) has examined the nature and frequency of fraudulent attacks on business-to-business payments as well as the industry fraud-risk tools that organizations use to control payments fraud. Continuing that research, in January 2009 AFP conducted its Payments and Fraud Control Survey to capture the payments fraud experiences of organizations during 2008.

The results of the *2009 AFP Payments Fraud and Control Survey* show that payments fraud is rampant: a majority of organizations experienced attempted or actual payments fraud in 2008. These results also underscore the importance of fraud control measures to mitigate risk and reduce exposure to losses from emerging assaults to payments.

AFP thanks JPMorgan for underwriting the *2009 Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, were 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 2009 AFP Payments Fraud and Control Survey include:

- Seventy-one percent of organizations experienced attempted or actual payments fraud in 2008.
  - Large organizations were more likely to have experienced payments fraud than were smaller ones. Eighty percent of organizations with annual revenues over \$1 billion were victims of payments fraud in 2008 compared with 63 percent of organizations with annual revenues under \$1 billion.
- Thirty percent of survey respondents report that incidents of fraud increased in 2008 compared to 2007.
  - Further, 38 percent of organizations experienced increased fraud activity during the second half of 2008 as economic conditions worsened in the U.S.
- Nine out of ten organizations (91 percent) that experienced attempted or actual payments fraud in 2008 were victims of check fraud. The percentage of organizations affected by payments fraud via other payment methods were:
  - ACH debit (28 percent)
  - Consumer credit/debit cards (18 percent)
  - Corporate/commercial cards (14 percent)
  - ACH credits (seven percent)
  - Wire transfers (six percent)
- Sixty-three percent of organizations that were victims of actual and/or attempted payments fraud in 2008 experienced no financial loss from payments fraud.
- Among organizations that did suffer a financial loss resulting from payments fraud in 2008, the typical loss was \$15,200.

### Fraud Control

- Organizations turn to a number of fraud control services provided by their banks, including:
  - Positive pay/reverse positive pay (82 percent)
  - ACH debit blocks (71 percent)
  - ACH debit filters (55 percent)
  - Payee positive pay (50 percent)
  - "Post no checks" restriction on depository accounts (34 percent)
- Organizations may opt out of particular fraud control services for a number of reasons: their management is confident that the organizations' internal processes are adequate (47 percent), the service is too expensive (20 percent), and/or the organization does not issue a sufficient number of checks (17 percent).
- Organizations can develop and/or modify internal business processes to mitigate potential payments fraud risks. Among the processes considered important include:
  - Stopped providing payment instructions by phone or fax (86 percent)
  - Increased use of electronic payments for business-to-consumer and business-to-business transactions (82 percent)
  - Reduced the number of bank accounts (82 percent)

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

### **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)
  - Altered payee names on checks issued by the organization (59 percent)
  - Altered employee pay checks (27 percent)
- Just under half of organizations that were victims of at least one attempt of check fraud during 2008 suffered a financial loss resulting from check fraud (47 percent).
- Twenty-two percent of organizations have been contacted by a third party claiming to be a holder in due course.
- Forty-seven percent of organizations that received at least one holder in due course claim did not pay a claimant because the check used for the claim was fraudulent.

### **ACH Fraud**

- Seventeen percent of organizations that were victims of ACH fraud during 2008 suffered a financial loss as a result.
- 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. Fifty-five percent of organizations did not use ACH debit blocks or ACH debit filters, and 36 percent did not use ACH positive pay.

### **Business-to-Business Card Payments Fraud**

- Seventy-eight percent of organizations that experienced fraud via the use of an organization's own corporate/commercial card indicate that the fraud was perpetrated by an external party.
  - Seventy percent of such organizations report that the fraud was committed by an unknown external party.
  - Eleven percent of such organizations indicate that the fraud was committed by a third-party, such as a vendor, professional services provider or business trading partner.
- Forty-four percent of organizations subject to corporate/commercial card fraud during 2008 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.

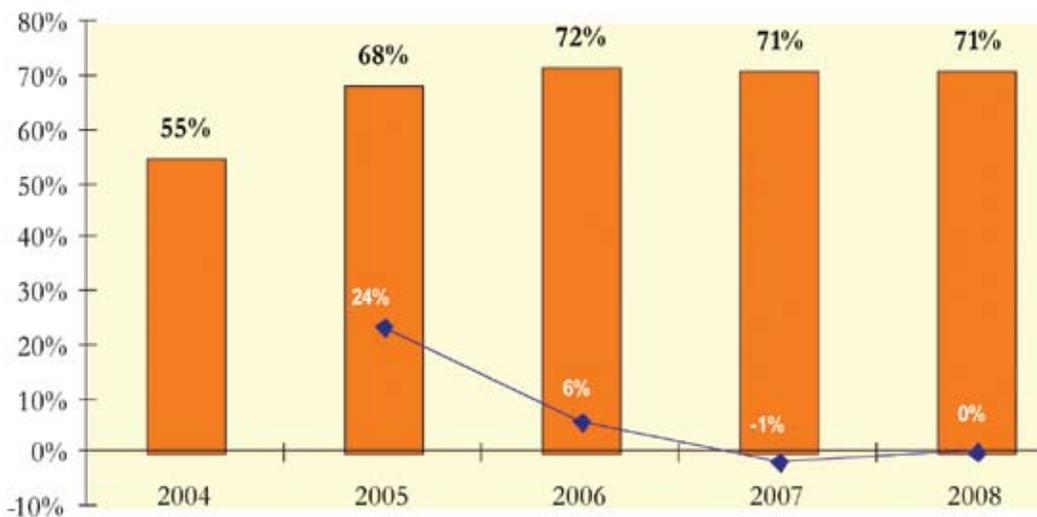
## Survey Findings

### Payments Fraud Overview

Payments fraud remained widespread during 2008. 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 demands a range of fraud-fighting tools and the constant vigilance of financial and treasury professionals responsible for protecting the assets of their organizations.

Almost three-quarters of organizations were victims of payments fraud in 2008. Seventy-one percent of organizations experienced attempted or actual payments fraud in 2008, a result that is similar to that found in the two previous annual AFP payments fraud surveys.

**Attempted or Actual Payments Fraud and Percentage Change From Previous Year**  
(Percent of Respondents)



Large organizations were more likely to have been the targets of payments fraud than were smaller organizations. Eighty percent of organizations with annual revenues over \$1 billion were victims of payments fraud in 2008 compared to 63 percent of organizations with annual revenues under \$1 billion.

**Organizations Subject to Attempted or Actual Payments Fraud in 2008**  
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization was a victim of payments fraud	71%	80%	63%
Organization was not a victim of payments fraud	29	20	37

Incidents of fraud increased for both large and small organizations in 2008 compared to 2007. Thirty percent of survey respondents report that incidents of fraud increased in 2008 compared to 2007, 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 2007 to 2008.

**Change in Prevalence of Payments Fraud in 2008 Compared to 2007**  
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Increased incidents of fraud	30%	31%	30%
About the same	55	54	56
Decreased incidents of fraud	15	15	14

The use of checks for payments is declining. According to *The 2007 Federal Reserve Payments Study* ([http://www.frbservices.org/files/communications/pdf/research/2007\\_payments\\_study.pdf](http://www.frbservices.org/files/communications/pdf/research/2007_payments_study.pdf)), more than two-thirds of all U.S. non-cash payments were made electronically during 2007. The number of checks used for payment fell by 7 billion between 2003 and 2006. Although the volume of checks is declining, checks are still the most widely used payment instrument for businesses. The *2007 AFP Electronic Payments Survey* found that 74 percent of business-to-business payments were made by checks.

But checks also continue to be the preferred target for criminals committing payments fraud. Nine out of ten organizations (91 percent) that experienced attempted or actual payments fraud in 2008 were victims of check fraud. This percentage is slightly lower than that reported for 2007 (94 percent).

**Prevalence of Attempted Fraud in 2008**  
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)

Payment Methods	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Checks	91%	94%	88%
ACH debits	28	28	28
Consumer credit/debit cards	18	15	19
Corporate/commercial purchasing cards	14	14	14
ACH credits	7	6	6
Wire transfers	6	4	5

Among organizations that experienced an increased incidence of payments fraud in 2008 compared to 2007, 82 percent indicate that check fraud increased over the past year. Eighteen percent report higher levels of consumer credit/debit card fraud and 14 percent report increased fraud involving ACH debits.

Electronic payments can offer organizations more fraud control. Survey respondents indicate that organizations were much less likely to be subject to fraud from electronic payments than from checks. Among organizations that were victims of attempted or actual payments fraud in 2008, 28 percent report ACH debit fraud in 2008, up slightly from 26 percent in last year's survey. The prevalence of fraud involving consumer credit/debit cards increased eight percentage points to 18 percent. The incidence of fraud via other payment methods was relatively unchanged from the previous year: 14 percent of organizations report corporate card fraud, seven percent report ACH credit fraud, and six percent report wire transfer fraud. The frequency of electronic payment fraud contrasts significantly with the nearly universal incidence of attempted or actual check fraud of greater than 90 percent.

The growth in check fraud has far outpaced the growth in electronic payments fraud. Of the organizations that experienced an increased number of fraud attempts during 2008, 82 percent report more check fraud while only 18 percent report more consumer credit/debit card fraud and just 14 percent more ACH fraud. However, large organizations with annual revenues over \$1 billion—which are more likely to make/use electronic payments—are also more likely to have experienced an increase in fraud from ACH debits and wire transfers. Fraud from accepting consumer credit/debit card payments was more likely to occur in small organizations (with annual revenues under \$1 billion) than in large organizations.

**Payment Methods Subject to More Payments Fraud in 2008 Compared to 2007**  
(Percent of Organizations Subject to Greater Amount of Attempted or Actual Payments Fraud in 2008)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Checks	82%	89%	76%
Consumer credit/debit cards	18	9	29
ACH debits	14	17	10
Corporate/commercial cards	11	9	10
Wire transfers	4	5	*
ACH credits	3	5	2

**Financial Loss from Fraud Attempts**

Although most organizations experienced attempted or actual payments fraud during 2008, the majority of them did not suffer financial loss from fraudulent activity. Sixty-three percent of organizations experienced no financial loss from payments fraud, while another 23 percent realized a financial loss of less than \$25,000 during 2008.

Even for those organizations that did suffer financial loss from payments fraud, the financial damages were relatively small. One likely reason is that financial institutions are subject to The Bank Secrecy Act of 1970, which requires them to track transactions that exceed \$10,000 to detect and prevent money laundering. As a result, it should be no surprise that 43 percent of organizations that suffered a financial loss due to payments fraud during 2008 suffered a financial loss resulting from payments of less than \$10,000.

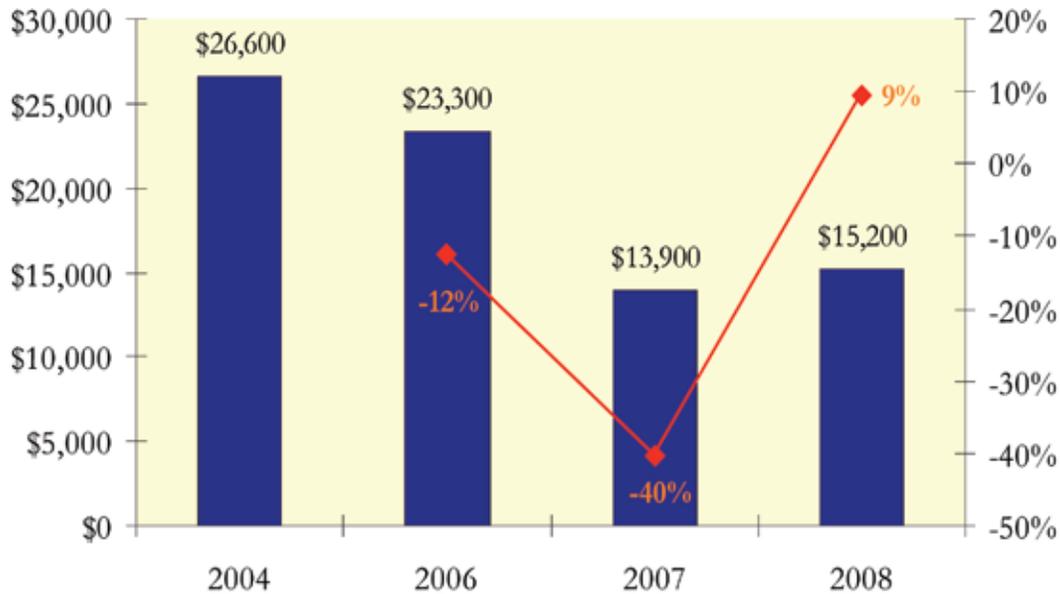
**Financial Loss Resulting from Payments Fraud in 2008**  
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
No loss	63%	67%	60%
Loss less than \$25,000	23	20	31
Loss between \$25,000 and \$49,000	5	5	2
Loss between \$50,000 and \$99,999	2	1	1
Loss between \$100,000 and \$249,999	4	3	4
Loss greater than \$250,000	3	4	2
Median financial loss*	\$15,200	\$15,900	\$10,000

\* - Of organizations that sustained financial losses resulting from payments fraud in 2008.

Organizations that sustained a financial loss resulting from payments fraud in 2008 reported a median financial loss from fraud of \$15,200. The typical loss for organizations with annual revenues greater than \$1 billion was 59 percent higher than that for smaller organizations—\$15,900 versus \$10,000. While the estimated median value of payments fraud steadily declined from 2004 to 2007, it increased from \$13,900 in 2007 to \$15,200 in 2008.

**Median Value of Payments Fraud and Percentage Change From Previous Year**



NOTE: 2005 Data was not captured.

Among the different payment methods, check fraud was the method most likely to result in financial losses to organizations. Sixty percent of organizations that sustained financial losses resulting from payments fraud indicate that checks were the payment form responsible for the greatest percentage of financial losses. Cards were the next most frequently cited payment method responsible for financial loss in 2008: 20 percent of organizations suffered financial loss from payments fraud via consumer credit/debit cards while ten percent of respondents report that corporate/commercial cards (e.g., purchasing cards and travel & entertainment (T&E) cards) were the method most responsible for financial losses sustained by their organizations resulting from payments fraud.

**Payment Method Most Responsible for Financial Loss Resulting from Fraud**  
(Percentage Distribution of Organizations Subject to Financial Losses Resulting from Payments Fraud in 2008)

Payment Methods	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Checks	60%	62%	55%
Consumer credit/debit cards	20	15	27
Corporate/commercial cards	10	9	13
ACH debits	5	7	6
ACH credits	3	6	*
Wire transfers	1	1	*

Economic conditions in the U.S. deteriorated significantly during the second half of 2008. Perhaps as a result of the economic slowdown, a significant number of organizations experienced an increase in payments fraud attempts during this period. Thirty-eight percent of organizations report an increase in payments fraud attempts in the second half of 2008, irrespective of industry sector. However, small organizations with revenues under \$1 billion experienced a higher incidence of fraud attempts – 41 percent – than did large organizations with revenues over \$1 billion – 34 percent.

**Increase in Payments Fraud Attempts During 2nd Half of 2008**  
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Increase in Fraud Attempts	38%	34%	41%
No increase in Fraud Attempts	62	66	59

**Fraud Control and Detection**

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 are positive pay and/or reverse positive pay that compares a company's record of checks issued with checks presented for payment to guard against fraudulent checks. Eighty-two percent of organizations use positive pay and/or reverse positive pay, including 87 percent of organizations with annual revenues greater than \$1 billion. Half of the organizations also protect against check fraud by using payee positive pay to circumvent the alteration of a payee name on checks. A third 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.

The increasing volume of ACH transactions for corporate payments not surprisingly also increases the potential for ACH fraud. Organizations can take advantage of a number of bank-provided fraud control services to protect against ACH fraud. Seven out of ten organizations use ACH debit blocks to prevent unauthorized ACH transactions, while 55 percent use ACH debit filters for pre-authorized ACH debits from known trading partners. Far fewer organizations (19 percent) use ACH positive pay, a dynamic fraud control tool which offers businesses the ability to evaluate ACH activity against established business rules to prevent unauthorized electronic debits. Universal Payment Identification Code (UPIC) which can be used to mask sensitive bank account information for ACH credits remains in its infancy, and only five percent of organizations report utilizing this method to combat ACH fraud. As with the services that protect against check fraud, large organizations are more likely to use ACH fraud prevention services than are smaller ones.

**Services 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	82%	87%	79%
	Payee positive pay	50	60	41
	"Post no checks" restriction on depository accounts	34	42	29
ACH	ACH debit blocks	71	79	60
	ACH debit filters	55	62	49
	ACH positive pay	19	19	18
	Universal Payment Identification Code (UPIC) for ACH credits	5	7	3
Other	Other	5	4	5

A small percentage respondents (five percent) indicate that their organizations do not use any of the fraud control services offered by their banks. Organizations eschew a particular fraud control service for a variety of reasons. Nearly half of the organizations decided not to use a particular payment fraud control service because they are confident that their internal processes provide adequate protection (47 percent). Twenty percent of organizations choose to not use certain fraud control measures because they consider the service too expensive; 17 percent of organizations do not issue enough checks to justify the expense. Large organizations are more likely to avoid using a particular service for reasons related to cost (30 percent) while smaller organizations do not use a service because they do not issue a sufficient number of checks (28 percent).

### Reasons for Not Using Fraud Control Services

(Percent of Organizations that Don't Use At Least One Bank Offered Fraud Control Service)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Use internal processes	47%	43%	51%
Service is too expensive	20	30	19
Company does not issue enough checks to justify service	17	7	28
Service is too difficult to use or too time consuming	16	17	19
Organization uses a different fraud control service	10	20	2
Bank does not provide the service	9	3	14
My bank will recover any losses	8	10	7
Other	12	10	12

In addition to purchasing fraud control services from their bank, many organizations develop their own internal measures and modify business processes to mitigate risk to payments fraud. Nearly nine out of ten 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. Eighty-six 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. Similarly, 82 percent of organizations that have increased their use of electronic payments for business-to-consumer and business-to-business transactions and reduced the number of bank accounts did so with fraud prevention in mind.

Other actions and/or business process changes considered important by organizations in reducing the organization's exposure to payments fraud risk include:

- Do not provide bank account number to payors for electronic payments (79 percent)
- Outsourced accounts payable (59 percent).

**Importance of Controlling Fraud in Decision to Take Particular Actions**  
(Percent of Organizations Taking Particular Action)

	Important	Somewhat Important	Not at all Important
Stopped giving payment instructions by phone or fax	48%	38%	14%
Increased use of electronic payments for B2C transactions (e.g., payroll cards, stored value cards, direct deposits to employee accounts)	46	36	18
Increased use of electronic payments for B2B transactions	45	37	18
Restricted the use of online data communication	43	46	11
Did not provide my bank account number to payors for electronic payments	34	45	21
Outsourced accounts payable	32	27	41
Reduced the number of bank accounts	31	51	19

One best practice of organizations 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. Seventy-one percent of organizations that maintain separate accounts have separate accounts for disbursement and collections while 60 percent of organizations separate bank accounts for checks and ACH payments. Just over two out of five organizations maintain separate accounts by payment type (e.g., vendor, tax, payroll, dividend). The decision to use separate bank accounts does not differ significantly by organization size.

**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	71%	73%	71%
Separate accounts for checks and ACH payments	60	63	57
Separate accounts by payment type (e.g., vendor, tax, payroll, dividend)	42	41	41
Separate account for wire transfers	37	40	31
Separate account for card payments	21	23	19
Other	5	5	3

One reason organizations separate their bank accounts by different payment methods and types is to reduce exposure to fraud. Fifty-four percent of respondents from organizations that maintain separate accounts believe that separate accounts are useful in preventing payments fraud. Another 36 percent believe that the use of separate accounts have been “somewhat” useful in the fight against payments fraud.

#### **Degree of Usefulness of Separate Accounts for Fraud Control**

(Percentage Distribution of Organizations that Maintain Separate Accounts for Different Payment Methods or Types)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Useful	54%	50%	59%
Somewhat useful	36	40	30
Not very useful	5	6	4
Unsure	5	4	7

#### **Check Fraud**

Checks remain the payment method targeted by most criminals to commit payments fraud. Seventy-two percent of organizations that were subject to check fraud in 2008 indicate that the fraud was perpetrated through the use of counterfeit checks using the organization’s MICR line data. Fifty-nine percent of organizations that were subject to check fraud in 2008 report that the criminals altered payee names on checks issued by the organization, while 27 percent of organizations subject to check fraud indicate that the fraud was targeted to employee paychecks.

#### **Types of Fraud Resulting from Using Checks**

(Percent of Organizations that Suffered Check Fraud in 2008)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Counterfeit checks (other than payroll) with the organization’s MICR line data	72%	75%	68%
Payee name alteration on checks issued	59	63	50
Loss, theft or counterfeit of employee paychecks	27	31	21
Other	7	5	12

Under half – 47 percent – of the organizations that were victims of at least one attempt of check fraud during 2008 suffered a financial loss resulting from that fraud. That percentage is up significantly from the 17 percent of organizations that reported a financial loss from check fraud in 2007. Large organizations were more likely to incur a financial loss from check fraud than were smaller organizations—50 percent of organizations with annual revenues greater than \$1 billion report sustaining a financial loss from check fraud in 2008 compared to 32 percent of organizations with annual revenues less than \$1 billion.

Organizations that incurred a financial loss resulting from check fraud identified a number of factors that led to the loss. Twenty-three percent of respondents indicate that the event involved internal fraud perpetrated by an employee of the organization. Twenty-one percent of organizations did not use payee positive pay while 20 percent did not use positive pay or reverse positive pay. Twenty percent of organizations did not reconcile their accounts on a timely basis while another 21 percent did not return checks on a timely basis.

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

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Resulted in financial loss	47%	50%	32%
Did not result in financial loss	53	50	68

A number of organizations experienced duplicate debits posted to their bank accounts as a result of a check having been deposited twice. Nearly a quarter of survey respondents indicate that their organization has been subject to duplicate debits, with equal proportions of large and smaller organizations reporting such activity at similar rates. In two-thirds of the occurrences, the duplicate debits were the result of operational error, but fraud was the cause 18 percent of the time. More than four out of five respondents (82 percent) from organizations that had duplicate debits indicate that the funds were credited back to their organizations' accounts on a timely basis—typically three days.

**Duplicate Debits Resulting from Checks Being Deposited Twice**  
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization had duplicate debits posted to an account because checks were deposited twice	23%	24%	23%
Organization did not have duplicate debits posted to an account because checks were deposited twice	77	76	77

Since 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. Nearly half of survey respondents indicate that their organizations transmit check images using remote deposit – an increase from 44 percent in 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 one percent of survey respondents whose organizations use remote deposit indicate their organization was the subject of 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
Experienced Fraud	1%	2%	1%
Did not Experience Fraud	99	98	99

An increasing concern for companies is “holder in due course” (HIDC) claims. A “holder in due course” is a third party that accepts and cashes a check in good faith without knowing that there was a problem with the check. The most common example of this is a check-cashing service that accepts a check unaware that a stop payment had been placed on the check.

Twenty-two percent of organizations have been contacted by a third party claiming to be a holder in due course. Large organizations were more likely to have been contacted by an alleged holder in due course than were smaller organizations. Twenty-five percent of respondents from organizations with annual revenues greater than \$1 billion indicate that their organizations have been contacted by a party claiming to be a holder in due course versus 16 percent of respondents from smaller organizations.

**Prevalence of Contact by “Holder in Due Course”**  
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Contacted by party claiming to be “holder in due course”	22%	25%	16%
Not contacted by party claiming to be “holder in due course”	78	75	84

Most organizations involved in HIDC claims had this happen multiple times during 2008. In the case of 12 percent of survey respondents, the organization was subject to potential holder in due course claims more than ten times during 2008. Only 22 percent of respondents report that their organizations had been contacted by a third party once during 2008 claiming to be a “holder in due course.” Twenty percent of large organizations were subject to “just” one holder in due course claim compared to a third of organizations with annual revenues below \$1 billion.

#### **Frequency of Contact by Holders in Due Course**

(Percentage Distribution of Organizations Contacted by Third Party Claiming to Be a Holder in Due Course)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
One time	22%	20%	32%
2-10 times	66	68	57
More than 10 times	12	12	11

In most cases, the holder in due course had a valid claim because the check was actually issued by the organization. However, more than half of organizations that were contacted by a holder in due course report that at least one claim was made with a counterfeit check. Fifty-three percent of respondents report that their organization received at least one holder in due course claim that involved a counterfeit check. Large organizations are more likely than smaller organizations to have received a holder in due course claim involving a counterfeit check: 63 percent of large organizations that were subject to a holder in due course claim in 2008 had at least one claim involving a counterfeit check versus 28 percent of similar smaller organizations.

If the check is counterfeit but is not an organization’s check, a person who accepts the check cannot make a holder in due course claim against the organization. If a check casher or other entity holding the check makes a claim for payment of a counterfeit check, the organization should reject the claim in writing. To protect itself against these fraudulent check claims, an organization should use positive pay or reverse positive pay and return the checks.

On the other hand, the organization is liable if it actually issues a second check to a dishonest payee who claims the original check was lost or stolen but later deposits or cashes both checks. In this case, the person who accepts the check is a holder in due course and has a valid claim against the organization despite the fact that a stop payment was placed on the check.

**Authenticity of Checks Used to Make Holder in Due Course Claims**  
(Percent of Organizations Contacted by Third Party Claiming to Be a Holder in Due Course)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Check was issued by my organization	76%	72%	86%
Counterfeit check	53	63	28
Other	1	*	3

Nearly half of organizations that received HIDC claims during 2008 did not honor the claim because the check used to make the claim was counterfeit. Forty-seven percent of organizations that received at least one holder in due course claim did not pay a claimant because the claim was made using a fraudulent check. Large organizations were more likely than their smaller counterparts to deny a claim based on a fraudulent check. Nearly three out of five organizations (57 percent) with annual revenues greater than \$1 billion did not pay on at least one holder in due course claim compared to 31 percent of smaller organizations. As of early 2009, 27 percent of organizations had not yet resolved at least one holder in due course claim made during 2008.

Forty-four percent of organizations did pay the full value of the check used in a holder in due course claim during 2008, but nine percent not only paid the full value of the check but also paid an additional fee. The typical organization that paid at least one holder in due course claim during 2008 sustained a loss of \$2,000 resulting from paying off the claim(s).

**Actions Taken in Dealing with Holder in Due Course**  
(Percent of Organizations who were contact by holder in due course)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Did not pay due to counterfeit check	47%	57%	31%
Paid full value of the check	44	46	43
Disputed holder in due course claim; resolution pending	27	25	29
Paid full value of the check plus a fee	9	6	14
Other	7	8	6

### ACH Fraud

ACH payments are one way of circumventing potential paper check fraud, and the practice of using ACH payments has increased significantly. According to NACHA, the number of ACH payments increased from 3.9 billion in 1996 to more than 18 billion in 2007, with transaction values almost tripling to \$32.9 trillion during the same period. But the increasing volume of ACH payments means an increased potential for ACH fraud. Although nearly a third of organizations were victims from at least one attempt of ACH fraud during 2008, just one in six organizations suffered a financial loss as a result. Seventeen percent of organizations – regardless of size – that were victims of ACH fraud during 2008 also suffered a financial loss.

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

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Resulted in financial loss	17%	18%	17%
Did not result in financial loss	83	82	83

### Managing ACH Fraud Risk

Organizations that suffered a financial loss as a result of ACH fraud generally did so because they did not follow best practices and/or execute their own business rules as expeditiously as they should have. Fifty-five percent of organizations that suffered a financial loss as a result of ACH fraud did not use ACH debit blocks or ACH debit filters while 36 percent did not use ACH positive pay. Of the organizations that did suffer losses from ACH fraud, 36 percent did so because ACH return was not timely, while for 18 percent the organization did not reconcile its accounts on a timely basis.

**Primary Reason the Organization Suffered Losses from ACH Fraud**  
(Percent of Organizations that Suffered a Financial Loss Resulting from ACH Fraud)

Did not use ACH debit blocks or ACH debit filters	55%
ACH return not timely	36
Did not use ACH positive pay	36
Account reconciliation not timely	18
Criminal take-over of my online system to initiate fraudulent transactions	18
Internal fraud (e.g., employee responsible)	9
Inaccurate key entry/error	9
Gaps in online security controls	9
Other	9

ACH's growing check conversion has resulted in permutations of check and ACH fraud. Savvy criminals are using fraudulent checks to originate ACH debits. Fifteen percent of organizations subject to ACH fraud in 2008 indicate that they initiated an ACH debit from an account listed on a fraudulent check.

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

Sixty-eight percent of respondents indicate that their organizations use corporate/commercial cards for business to business payments. Purchasing cards are the most likely instruments of corporate/commercial cards (76 percent), followed by travel and entertainment (T&E) cards (51 percent), and ghost or virtual cards (25 percent). Fourteen percent of organizations were subject to actual or attempted payments fraud in 2008 using corporate/commercial cards. Sixty-nine percent of these organizations experienced fraud using the organizations' own corporate/commercial cards.

#### **Fraud Resulting from Organizations' own Corporate/Commercial Cards**

(Percentage Distribution of Organizations that experience fraud associated with Corporate/Commercial Cards)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Experienced fraud impacting organization's own corporate/commercial cards	69%	69%	63%
Did not experience fraud impacting organization's own corporate/commercial cards	31	31	37

Typically, payments fraud involving an organization's own corporate/commercial cards is committed by an outside party. Seventy percent of organizations that were subject to fraud committed using an organization's own corporate/commercial card indicate that the fraud was perpetrated by an unknown external party, while 11 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. A third of organizations were subject to fraud by its own employees using corporate/commercial cards.

#### **Primary Party Responsible for Fraud Using Organizations' Corporate/Commercial Cards**

(Percent of Organizations that Suffered Attempted or Actual Fraud Using Organizations' Corporate/Commercial Cards)

<b>Outside</b>	Unknown external party	70%
	Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	11
<b>Internal</b>	Employee	32
<b>Other</b>	Other	3

When an organization’s own checks were used to perpetrate fraud, those incidents frequently did not result in financial liability to the organization. But the opposite is true in those cases of fraud committed via corporate/commercial cards. Forty-four of organizations that were subject to corporate/commercial card fraud during 2008 suffered actual financial losses resulting from the fraud. Other parties that suffered financial loss as a result of corporate/commercial card fraud include the merchant where the card was used (42 percent) and the bank or financial institution that issued the card (33 percent).

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

My organization	44%
Merchant	42
Card issuing bank	33
Card processor	14
No organization suffered financial loss	11
Other	14

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

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.

**Financial Loss Due to Accepting Corporate/Commercial Cards in 2008**  
 (Percentage Distribution of Organizations that Experienced Fraud Associated with Accepting Corporate/Commercial Cards)

Experienced financial loss	17%
Did not experience financial loss	83

When an organization suffers a financial loss resulting from accepting a fraudulent B2B card payment, it is often because it failed to follow processes that would likely have prevented the fraudulent activity. Eighty-three percent 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 the organization suffered a financial loss from a fraudulent card transaction include:

- Failure to authenticate the cardholder (50 percent)
- Failure to respond to a chargeback 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 B2B Card Payments)

Card-not-present merchant assumes liability	83%
Did not authenticate cardholder (e.g., cardholder's address)	50
Delayed chargeback response	33
Other	33

## Conclusion

Payments fraud is pervasive. The majority of organizations (71 percent) surveyed experienced attempted or actual payments fraud in 2008, and 30 percent report that incidents of fraud increased last year compared with the number of incidents in 2007. Of those companies that experienced some payments fraud, 37 percent suffered actual financial losses, with a median loss of \$15,200. Those companies that avoided financial loss did so mainly through the use of defenses available from financial institutions and by following best practices.

Economic pressures may have led to a potential increase in fraud attempts during the second half of 2008, illustrated by the increase in the median value of payments fraud from \$13,900 in 2007 to \$15,200 in 2008, and 38 percent increase in fraud attempts in the second half of the year. Nevertheless, the losses resulting from payments fraud remain relatively small.

Fraudsters tend to migrate to the least resistant path or product. Among payment methods, these continue to be checks. Although the volume of check payments has been declining, check payment fraud is still the most frequent type of fraud suffered by organizations. Sixty percent of organizations report that this payment method was most responsible for financial loss from fraud.

An increasing issue for organizations is check fraud based on “holder in due course” (HIDC) claims – a claim to be paid by a third party that accepts and cashes a check in good faith without knowing that there is a problem with the check. In 2008, 22 percent of companies had been contacted by a third party claiming to be a “holder in due course.” In more than two-thirds of the cases, the check was issued by the organization while 53 percent involved a counterfeit check. If the check is counterfeit – a fraudulent item that was not issued by the organization – the check casher has no claim to be a holder in due course against the company and the company is not liable. However, if the organization issued the check, the person who accepts the check can be a holder in due course and the claim is valid.

Accordingly, to protect against check fraud as well as holder in due course claims for fraudulent checks, prudent organizations use positive pay or reverse positive pay. Eighty-two percent of companies surveyed report using positive pay or reverse positive pay. Companies have also increasingly employed other check fraud control measures. The use of payee positive pay to detect payee name alternation has grown significantly in the last four years, from a third of organizations using the service in 2004 to half of the organizations using it in 2008.

The rights of a holder in due course are defined by the Uniform Commercial Code (UCC), Articles 3 and 4, which establish the negotiability of checks and the certainty of payment. Organizations should be aware of the risks and explore the options when issuing duplicate checks to payees. They should also reject HIDC claims when they are based on fraudulent items.

The increasing use of electronic payments, specifically ACH to make payments, is expected to reduce exposure to fraud. Indeed, among organizations that were victims of attempted or actual payments fraud in 2008, 28 percent reported ACH debit fraud in 2008.

Traditionally low-risk, the ACH network has recently expanded to include more participants, continuously changing relationships, new types of non-recurring payments (e.g., telephone and Web-initiated ACH transactions) and greater risks. With the broad changes underway in the payments system, the ACH channel is becoming an attractive target for fraud. The primary reason that organizations suffered a financial loss from ACH fraud in 2008 was lack of effective security measures that include ACH debit blocks or ACH debit filters (55 percent), and ACH positive pay (36 percent).

Financial liability from ACH fraud, however, was fairly low (17 percent) because corporate businesses implemented effective fraud detection and risk mitigation strategies. Adding internal controls and procedures help prevent electronic payments fraud. Strategies include reconciling accounts more frequently, improving the timely return of payments, adding or revising approvals of electronic payments and auditing payment processes more frequently.

Risk and fraud factors have increased alongside ACH's growing check conversion and electronic payments volume. With the convergence of check and ACH, the manipulation of check and ACH transactions is an increasing concern. Nearly 15 percent of organizations that received fraudulent ACH transactions were passed through fraudulent checks that would have been stopped by check-based positive pay ledgers but instead were presented as ACH debits. The experience highlights the need for tighter fraud control in this area.

Corporate/commercial cards are a significant source of fraud reported by organizations. The illicit use of card data by an external party – an unknown source, data exposure by a third-party or outsourcer responsible for customer data – was the primary cause in 78 percent of corporate/commercial card fraud incidents. The percentage of incidents where an unknown external party was responsible for fraud increased from 61 percent in 2007 to 70 percent in 2008. However, malicious intent by a company insider or employee accounted for 32 percent of such fraud.

Perpetrators of fraud are continually looking for ways to outsmart the system and are becoming increasingly savvy and creative. As business customers move toward more electronic payment vehicles – like ACH and cards – fraudsters will make these their channels of choice unless fraud prevention practices and safeguarding tools hinder their path. Using fraud detection best practices and services can reduce an organization's exposure to check, ACH and other forms of payments fraud. The Association for Financial Professionals continues to promote the awareness of fraud issues and encourage the use of best practices by treasury and finance professionals by keeping them continually informed about the prevalence, methods and prevention of payments fraud through regular surveys on the issue.

## About the Respondents

On January 8, 2009, the Research Department of the Association for Financial Professionals (AFP) surveyed 5,300 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, directors, assistant treasurers and controllers. After eliminating surveys sent to invalid and/or blocked email addresses, the 490 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 139 responses. The following tables provide a profile of the survey respondents.

### Annual Revenues (Percentage Distribution)

Under \$50 million	6%
\$50-99.9 million	4
\$100-249.9 million	9
\$250-499.9 million	10
\$500-999.9 million	16
\$1-4.9 billion	31
\$5-9.9 billion	10
\$10-20 billion	7
Over \$20 billion	7

### Industry Classification (Percentage Distribution)

Manufacturing	17%
Energy (including utilities)	13
Retail (including wholesale/ distribution)	12
Government	9
Insurance	8
Health services	7
Non-profit (including education)	6
Banking/Financial services	5
Business services/Consulting	4
Real estate	4
Transportation	4
Construction	3
Software/Technology	3
Telecommunications/Media	3
Hospitality/Travel	2

**Ownership Type**  
(Percentage Distribution)

Publicly owned	48%
Privately held	32
Non-profit (non-for-profit)	9
Government (or government owned entity)	11

Financial professionals who responded to the survey represent organizations that accept and make payments using a variety of payment methods.

**Methods Used to Make and/or Receive Payments**  
(Percent of Respondents)

Payment Methods	All Organizations	Revenues over \$1 billion	Revenues under \$1 billion
Checks	97%	98%	99%
Wire transfers	96	99	95
ACH credits	90	96	91
ACH debits	83	84	85
Corporate/commercial cards	75	76	61
Consumer credit/debit cards	49	49	52

AFP thanks JPMorgan for underwriting the *2009 Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, were the sole responsibility of the AFP Research Department.

**AFP Research**

AFP Research provides financial professionals with proprietary and timely research that drives business performance. The AFP Research team is led by Director of 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](http://www.AFPonline.org/research).

**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](mailto:AFP@AFPonline.org)

Web Site                [www.AFPonline.org](http://www.AFPonline.org)

Phone                    301.907.2862