Association for Financial Professionals®

2008 AFP Payments Fraud and Control Survey

Report of Survey Results

Underwritten by

EPN®

2008 AFP Payments Fraud and Control Survey

Report of Survey Results

March 2008

Underwritten by Electronic Payments Network (EPN)

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

Payments Fraud and Control Survey
Introduction

Safeguarding their organizations against payments fraud continues to be a major concern of treasury and finance professionals. Repeated reports of check scams, data breaches and losses from online commerce reinforce the need to strengthen defenses against attempted fraud.

In January 2008, the Association for Financial Professionals (AFP) conducted a survey to spotlight the type and frequency of payments fraud experienced by organizations in 2007. The survey was a follow-up to similar AFP surveys conducted in each of the previous three years to measure the prevalence of payments fraud and the weapons that organizations deploy to defend against it.

This year's survey sought to reveal the gaps in payment systems defenses that resulted in financial liability for some organizations and the fraud control measures that other organizations use to prevent financial losses from payments fraud. Responses to the survey would identify best practices that protect organizations against fraud in check, ACH and card payments from both internal and external sources. The survey was also designed to focus attention on the security measures that organizations are adopting to protect online payments and cash management data.

AFP thanks the Electronic Payments Network (EPN) for underwriting the 2008 Payments Fraud and Control Survey. Both questionnaire design and the final report were the responsibility of the AFP Research Department, which is solely responsible for the content and conclusions.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Highlights of Survey Results

The key findings of the 2008 AFP Payments Fraud and Control Survey include:

- Seventy-one percent of organizations experienced attempted or actual payments fraud in 2007
  - Eighty percent of organizations with annual revenues greater than $1 billion were victims of payments fraud in 2007.
  - Fifty-eight percent of organizations with annual revenues under $1 billion were victims of payments fraud in 2007.
- Almost all organizations (94 percent) that experienced attempted or actual payments fraud in 2007 were victims of check fraud.
  - Organizations were much less likely to be subject to fraud from electronic payments than from checks, including:
    - ACH debit (26 percent)
    - Corporate cards (13 percent)
    - ACH credit (four percent)
    - Wire transfer (three percent).
  - Sixty-three percent of organizations subject to payments fraud suffered no financial loss resulting from the fraud.
  - Even among organizations that were subject to financial losses from payments fraud, the financial damages were relatively small—the typical financial loss was $13,900.

Check Fraud

- Among the types of accounts subject to check fraud, accounts payable/disbursement accounts were the most frequent targets (84 percent).
  - The second most frequent target of check fraud was the payroll account (34 percent).
- Tight internal controls and positive pay services ensure that organizations do not suffer financial losses from check fraud. Defenses include:
  - Positive pay or reverse positive pay (77 percent)
  - Daily reconciliation (45 percent)
  - Internal controls (e.g., separation of duties) (43 percent)
  - Payee positive pay (40 percent).

ACH Fraud

- Fifteen percent of organizations experienced financial losses from ACH fraud in 2007.
- Failure to adopt effective internal procedures and bank fraud control services were the most frequently cited reasons for the loss, including:
  - Not reconciling accounts or returning fraudulent ACH debits on a timely basis (56 percent).
  - Not using ACH debit blocks or ACH debit filters (50 percent)
  - Not using ACH positive pay (19 percent)
  - Failing to prevent internal fraud (19 percent).
- ACH fraud control best practices include:
  - ACH debit blocks (76 percent)
  - Daily reconciliation (72 percent)
  - ACH debit filters (64 percent)
  - Timely ACH return (50 percent).

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Online Payments Fraud Control

- To avert hacker attacks, data breaches, and internal fraud, organizations have put in place a number of practices to protect their online payments and cash management data, including:
  - Segregating responsibilities among different employees for payments template maintenance, payments entry and payments approval (88 percent)
  - Using multi-factor authentication tools, e.g., tokens, digital certificates, smart cards (87 percent)
  - Deleting online user IDs as part of the exit procedure when employees leave (83 percent)
  - Assigning dual system administrators for online cash management services (82 percent)
  - Requiring online passwords be changed periodically (82 percent).

Business-to-Business Card Payments Fraud

- Only 13 percent of organizations that use corporate cards report that they experienced attempted or actual payments fraud through the use of these cards.
- Techniques used to mitigate fraudulent use of corporate cards include:
  - Requiring original receipts for purchases and/or print-outs of Web confirmations of purchases (78 percent)
  - Defining card spending limits by employee and by employee level; not the same for all employees (68 percent)
  - Assigning a permanent administrator to train cardholders and monitor usage (67 percent)
  - Developing a detailed cardholder agreement that both cardholders and supervisors must sign (54 percent).

Consumer Electronic Payments Fraud

- Ten percent of organizations that accept electronic payments from consumers indicate that they were victims of attempted or actual consumer ACH and/or card payments fraud in 2007.
  - Among payment forms targeted:
    - Credit cards (89 percent)
    - ACH (38 percent)
    - Signature debit cards (24 percent).

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Survey Findings

Payments Fraud Overview

Payments fraud continued at high levels in 2007. The vulnerability of all payment methods—especially checks—to fraud from external and internal sources calls for a range of fraud-fighting tools and the constant attention of financial professionals responsible for protecting the assets of their organizations.

Almost three-quarters of organizations were victims of payments fraud in 2007. Seventy-one percent of organizations experienced attempted or actual payments fraud in 2007, a result virtually unchanged from the 72 percent reported in last year's AFP survey.

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 2007 compared with 58 percent of organizations with annual revenues under $1 billion.

Organizations Subject to Attempted or Actual Payments Fraud in 2007
(Percentage Distribution)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Organization was a victim of payments fraud	71%	80%	58%
Organization was not a victim of payments fraud	29	20	42

Fraud increased at both large and small organizations in 2007 compared to that reported in 2006. Almost one-third of survey respondents report that incidents of fraud increased in 2007 compared to 2006, while only 18 percent indicate that the number of incidents declined. The remaining 52 percent of respondents experienced no significant change in payments fraud activity from 2006 to 2007.

Change in Number of Payments Fraud Attempts in 2007 Compared to 2006
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Increased incidents of fraud	30%	30%	30%
About the same	52	52	51
Decreased incidents of fraud	18	18	19

©2008 Association for Financial Professionals, Inc. All Rights Reserved

Checks continue to be the preferred target for criminals committing payments fraud. Almost all organizations (94 percent) that experienced attempted or actual payments fraud were victims of check fraud in 2007. This percentage is relatively unchanged from that reported for 2006. Moreover, among organizations that reported more fraud in 2007 than in the previous year, 90 percent indicate that checks were the cause, versus 71 percent in 2006.

The widespread prevalence of check fraud is occurring despite a significant decline in check usage nationwide. According to the latest Federal Reserve study of U.S. noncash payments, check volume decreased by an annual average of 6.4 percent between 2003 and 2007, driven in part by an explosion in consumer debit card use. According to *AFP's Electronic Payments Survey*, although the majority of business-to-business (B2B) payments continue to be made by check, organizations are increasingly using electronic payment methods for transactions with trading partners.

Moving from checks to electronic payments can be a fraud-fighting tool. Organizations are 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 2007, 26 percent report ACH debit fraud in 2007, down from 35 percent reported in last year's survey. Fraud against other payment methods was relatively unchanged from the previous year: 13 percent report corporate card fraud, four percent report ACH credit fraud and only three percent report wire transfer fraud. These results contrast with the nearly universal incidence of attempted or actual check fraud.

Payment Methods Subject to Attempted or Actual Payments Fraud in 2007
(Percent of Organizations Subject to Attempted or Actual Payments Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Checks	94%	96%	90%
ACH debits	26	31	22
Corporate cards	13	13	13
Consumer ACH and/or card payments#	10	10	13
ACH credits	4	3	6
Wire transfers	3	4	*
Prepaid/gift cards	1	1	2

Receive only

The growth in check fraud has far outpaced the growth in electronic payments fraud.
Of the organizations experiencing more fraud attempts in 2007 than in 2006, 90 percent report more *check* fraud while only 16 percent report more *ACH* fraud. However, large organizations with annual revenues over $1 billion—which are more likely to use electronic payments—were also more likely to have experienced an increase in fraud from ACH debits and corporate cards. Fraud from accepting consumer ACH and/or card payments was more likely to hit organizations with annual revenues under $1 billion.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Payment Methods Subject to More Payments Fraud in 2007 Compared to 2006
(Percent of Organizations Subject to Greater Amount of Attempted or Actual Payments Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Checks	90%	88%	89%
ACH debits	16	20	11
Consumer ACH and/or card payments#	10	8	17
Corporate cards	9	11	6
Wire transfers	2	2	*
Prepaid/gift cards	1	2	*
ACH credits	1	*	3

#receive only

Although most organizations experienced attempted or actual payments fraud in 2007, 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 25 percent realized financial loss of less than $25,000.

Even for those organizations that were subject to financial loss from payments fraud, the financial damages were relatively small. The median financial loss from fraud in 2007 was $13,900. The typical loss for organizations with annual revenues greater than $1 billion was more than double that of smaller organizations—$18,200 versus $8,200.

Financial Loss Resulting from Payments Fraud in 2007
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
No financial loss	63%	63%	66%
Less than $10,000	17	13	21
$10,000-$24,999	8	10	6
$25,000-$49,999	4	3	4
$50,000-$99,999	3	3	1
$100,000-$249,999	3	4	1
$250,000 and above	4	4	1
Median loss#	$13,900	$18,200	$8,200

#Among organizations subject to financial losses resulting from fraud in 2007

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Check Fraud

Despite the widespread prevalence of check fraud, most organizations did not suffer a financial loss, although the time and expense of defensive measures is also a financial consideration. Most organizations that were victims of attempted or actual check fraud in 2007 were not financially liable for that fraud. Only 17 percent of organizations suffered financial losses, down from 25 percent that reported a financial loss from check fraud in 2006. Large organizations with annual revenues greater than $1 billion were more likely to have sustained financial losses from check fraud than were smaller organizations (18 percent versus 12 percent).

Financial Loss Resulting from Check Fraud in 2007
(Percentage Distribution of Organizations Subject to Check Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Organization suffered financial loss	17%	18%	12%
Organization did not suffer financial loss	83	82	88

Among the types of accounts subject to check fraud, accounts payable/disbursement accounts were the most frequent targets. Eighty-four percent of organizations report that these accounts were hit; and there was little difference between large and small organizations. The second most frequent target of check fraud was the payroll account, experienced by 34 percent of organizations. However, large organizations with annual revenues over $1 billion were twice as likely to be victims of payroll account fraud than were smaller organizations (40 percent versus 21 percent). This may be due to the fact that large organizations are likely to have more employees than smaller ones and thus disburse a larger volume of payroll checks. Fifteen percent of organizations report check fraud that targeted their depository accounts.

Types of Accounts Subject to Check Fraud
(Percent of Organizations Subject to Check Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Accounts payable/disbursement	84%	84%	83%
Payroll	34	40	21
Depository	15	15	12
Dividend	1	1	1
Tax	1	1	*
Other	8	7	8

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Failure to enforce internal controls or adopt commonly used fraud defenses were the major reasons that organizations suffered financial losses from check fraud. One-quarter of organizations attributed financial losses to their failure to reconcile accounts or return checks on a timely basis. Internal fraud—caused by an employee, for example—was responsible for financial losses at two out of five organizations.

Use of positive pay or reverse positive pay is recommended as a payments best practice. Payee positive pay, which protects against altered payee names, is another best practice. Last year's AFP payments fraud survey revealed that almost two-thirds of check fraud victims experienced altered payee names on the checks they issued. Nineteen percent of organizations suffering financial losses from check fraud in 2007 failed to use payee positive pay, and 13 percent did not use positive pay/reverse positive pay.

Other reasons for financial loss from check fraud include the receipt of fraudulent checks from customers.

Reasons Organization Suffered Financial Loss from Check Fraud
(Percent of Organizations Subject to Financial Loss from Check Fraud)

Account reconciliation and/or check return not timely	26%
Internal fraud (e.g., employee responsible)	20
Did not use payee positive pay	19
Did not use positive pay/reverse positive pay	13
Did not timely process positive pay exception items	*
Other	48

Check fraud control best practices

Tight internal controls and positive pay services ensured that organizations did not suffer a financial loss from check fraud in 2007. Over three-quarters of organizations report that positive pay or reverse positive pay was responsible for preventing financial loss from check fraud. Payee positive pay prevented check fraud loss at 40 percent of organizations. These services combined with internal controls to stop the financial drain of check fraud. More than two out of five organizations indicate that daily reconciliation and internal controls such as separation of duties prevented financial loss.

Because depository accounts were also hit by check fraud, a "post no checks" restriction on depository accounts is often useful. The service stopped check fraud from causing losses at 21 percent of organizations, especially those with annual revenues over $1 billion.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Fraud Control Measures Responsible for Preventing Financial Loss from Check Fraud
(Percent of Organizations Not Subject to Financial Loss from Check Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Positive pay/reverse positive pay	77%	76%	77%
Daily reconciliation	45	46	42
Internal controls (e.g., separation of duties)	43	46	36
Payee positive pay	40	49	24
"Post no checks" restriction on depository accounts	21	26	12
Timely check return	16	14	22
Other	9	8	9

Payee positive pay

Payee positive pay is a key defensive weapon against check fraud. It enables organizations to view the payee name on potentially fraudulent positive pay exception items before deciding whether to pay or return the check. While the use of payee positive pay has increased among organizations that experienced check fraud, smaller organizations – those with annual revenues under $1 billion – have not adopted the service as extensively as larger organizations have. Sixty-four percent of organizations with annual revenues greater than $1 billion use payee positive pay. While just 51 percent of smaller organizations use the service, adoption by smaller organizations did pick up in 2007.

Use of Payee Positive Pay
(Percentage Distribution of Organizations Subject to Check Fraud in 2007)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Started using payee positive pay in 2007	13%	10%	20%
Started using payee positive pay before 2007	47	54	31
Do not use payee positive pay	40	36	49

Remote deposit

The growing use of remote deposit services has not resulted in check fraud. Although 44 percent of organizations that experienced payments fraud in 2007 use remote deposit to image checks at their own locations for transmission to their bank, only one survey respondent reported check fraud associated with the service.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Employee pay checks

More than one in five organizations that were victims of check fraud experienced fraud resulting from the loss, theft or counterfeit of employee pay checks. Pay check fraud was a more frequent occurrence at organizations with annual revenues over $1 billion than at smaller organizations (24 percent versus 17 percent).

Prevalence of Fraud Resulting from Loss, Theft or Counterfeit of Employee Pay Checks
(Percentage Distribution of Organizations Subject to Check Fraud in 2007)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Subject to fraud from employee pay checks	22%	24%	17%
Not subject to fraud from employee pay checks	72	70	79
N/A	6	6	4

However, smaller organizations were more likely than larger ones to have experienced more pay check fraud in 2007 than in the previous year. Thirty-nine percent of organizations with annual revenues under $1 billion and 18 percent of larger organizations report greater incidents of pay check fraud in 2007 than in 2006.

Change in Prevalence of Fraud Resulting from Loss, Theft or Counterfeit of Employee Pay Checks in 2007 Compared to 2006
(Percentage Distribution of Organizations Subject to Check Fraud from Loss, Theft or Counterfeit of Employee Pay Checks)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
More fraud in 2007	26%	18%	39%
About the same	62	62	61
Less fraud in 2007	12	18	*

Payroll best practices

Offering employees direct deposit of pay and payroll cards are considered best practices for reducing fraud associated with employee pay checks. Positive pay and ACH debit blocks are often used as reinforcements. The comments of survey respondents are testimony to the value of electronic payments for payroll.

- *98% of our employees are enrolled in our direct deposit program. We are experiencing maximum effectiveness in reducing fraudulent paycheck activity as a result.*

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

- *All of our employees are on direct deposit and it has eliminated all fraud associated with pay checks.*
- *Our organization is very aggressive in encouraging all employees to use direct deposit but it is not mandated. Payroll check fraud is minimal for us but all attempts have been caught by positive pay.*
- *Direct deposit helps by eliminating checks in circulation, but payee positive pay is the best deterrent.*
- *Direct deposit and payroll cards have reduced the number of employee pay checks written, thus reducing the chances of fraud.*
- *You need to make sure that you have an ACH block on your payroll files so that only people authorized to debit your account do so. In the past, we had a former employee attempt to use payroll account information from the bottom of his check to make electronic bill payments to cover his bills after he was no longer employed with us.*

ACH Fraud

As in the case of check fraud, most organizations that experienced ACH fraud did not suffer financial loss as a result of the fraud. Only 15 percent of organizations experienced financial loss from ACH fraud in 2007, down from 20 percent reported in 2006 and 25 percent in 2005.

Financial Loss Resulting from ACH Fraud in 2007
(Percentage Distribution of Organizations Subject to ACH Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Organization suffered financial loss	15%	17%	14%
Organization did not suffer financial loss	85	83	86

Failure to adopt effective internal procedures and bank fraud control services were the most frequently cited reasons for the financial loss. Fifty-six percent of organizations that suffered financial losses from ACH fraud did not reconcile their accounts or return fraudulent ACH debits on a timely basis. Half of organizations experienced financial losses because they did not use ACH debit blocks or ACH debit filters. Nineteen percent did not use ACH positive pay.

NACHA rules require that unauthorized or improper corporate debits be returned in time to be received by the originating bank "no later than the opening of business on the second banking day following the Settlement Date of the original entry." In effect, organizations have one day to return an ACH debit. Timely reconciliation and processing are critical.

Other deficiencies in internal procedures causing financial loss include internal fraud, key entry errors and gaps in online security controls.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Reasons Organization Suffered Financial Loss from ACH Fraud
(Percent of Organizations Subject to Financial Loss from ACH Fraud)

Account reconciliation and/or ACH return not timely	56%
Did not use ACH debit blocks or ACH debit filters	50
Internal fraud (e.g., employee responsible)	19
Did not use ACH positive pay	19
Inaccurate key entry/error	13
Gaps in online security controls	6
Other	13

ACH fraud control best practices

Despite having been victims of attempted ACH fraud, organizations did not suffer financially because they were protected by their bank's anti-fraud services and by implementing tight internal controls. Three-quarters of organizations (76 percent) indicate that ACH debit blocks prevented financial loss from ACH fraud and 64 percent credit ACH debit filters with their defense. Large organizations with annual revenues over $1 billion are much more likely to credit ACH debit blocks and ACH debit filters with preventing financial loss than are smaller organizations. Nevertheless, over half of smaller organizations (60 percent) report that ACH debit blocks helped them avoid losses.

The internal defense most frequently cited as responsible for preventing financial losses from ACH fraud is daily reconciliation. Seventy-two percent of organizations, especially those with annual revenues under $1 billion, indicate that daily reconciliation prevented loss of funds.

Other internal controls that proved effective in preventing financial loss include:

- Timely ACH return (50 percent)
- Using separate accounts for checks and ACH payments (31 percent)
- Separating accounts by payment type (21 percent)
- Online security controls (19 percent).

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Fraud Control Measures Responsible for Preventing Loss from ACH Fraud
(Percent of Organizations Not Subject to Financial Loss from ACH Fraud)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
ACH debit blocks	76%	81%	60%
Daily reconciliation	72	71	76
ACH debit filters	64	68	48
Timely ACH return	50	51	52
Separate accounts for checks and ACH payments	31	32	24
Separate accounts by payment type	21	14	40
Online security controls	19	17	24
ACH positive pay	2	2	4
Other	5	3	8

Criminals have used information from the MICR line of checks to originate fraudulent ACH debits. Twenty-two percent of organizations that were subject to ACH fraud in 2007 indicate that fraudulent ACH debits to their accounts were based on checks that were converted to ACH debits. Another 30 percent received fraudulent ACH debits but were uncertain whether converted checks were the source.

Online Payments Fraud Control: Best Practices

News headlines reporting hacker attacks, data breaches and internal fraud have heightened the awareness of all organizations to the vulnerability of online payments and cash management data. Most organizations, both large and small, have adopted multiple defensive measures against internal and external fraud. More than four out of five organizations take the following actions:

- Segregate responsibilities among different employees for payments template maintenance, payments entry and payments approval (88 percent)
- Use multi-factor authentication tools, e.g., tokens, digital certificates, smart cards (87 percent)
- Delete online user IDs as part of the exit procedure when employees leave (83 percent)
- Assign dual system administrators for online cash management services (82 percent)
- Require that online passwords be changed periodically (82 percent).

Other controls are used somewhat less frequently. Slightly more than half of organizations periodically evaluate employee job functions to remove online services and establish different payment transaction limits for employees based on job level and responsibilities.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Security Measures Adopted to Protect Online Payments and Cash Management Data
(Percentage Distribution)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Segregate responsibilities among different employees for payments template maintenance, payments entry and payments approval	88%	91%	85%
Use multi-factor authentication tools offered by the bank, e.g., tokens, digital certificates, smart cards	87	91	82
Delete online user IDs as part of the exit procedure when employees leave	83	85	78
Assign dual system administrators for online cash management services	82	86	76
Require that online passwords be changed periodically	82	83	79
Periodically evaluate employee job functions and remove online services	59	59	58
Establish different transaction limits for employees that initiate and approve online payments based on their job level and responsibilities	56	55	56
Set up alerts to notify managers of payments initiated above a threshold amount that should warrant management attention	24	20	28

Comments of survey respondents testify to the effectiveness of these online security measures and the value of multiple layers of protection.

- *Online security measures are effective in preventing and detecting payment fraud. Also, the use of digital certificates prevents users from sharing passwords and/or rights, which was common in the old PC-based systems.*
- *We embrace any technology that makes it difficult to commit fraud. We do sacrifice some efficiency but it helps to control fraud. This is a change from our past where we would place efficiency first. Safety is now number one.*
- *I feel the more dual control and restricted access to systems, the better for all.*
- *Online security measures have lowered our risk of fraud and allow for real-time alerts and responses.*

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

- *Online security measures are very effective. Combined with daily reconciliation, online security measures have allowed our company to detect fraud and then prevent losses to the company.*
- *Security measures have been effective - no fraud on our accounts. We also utilize payee positive pay for the checks we issue and we try to move more payments to electronic.*

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

Seventy-three percent of respondents indicate that their organizations use corporate cards. However, only 13 percent of these organizations report that they experienced actual or attempted payments fraud through use of corporate cards.

Purchasing cards were more likely to have been the instruments of corporate card fraud than were travel and entertainment (T&E) cards (75 percent versus 46 percent). Unknown external parties or employees were most likely to have been the perpetrators of corporate card fraud.

Party Responsible for Corporate Card Fraud in 2007
(Percent of Organizations Subject to Corporate Card Fraud When Making B2B Payments)

Unknown external party	61%
Employee	50
Vendor	14

While the majority of organizations did not suffer financial losses as a result of corporate card fraud, the percentage that did experience losses (33 percent) was higher than for other methods of payment. Parties that shared liability for financial losses from corporate card fraud include the card issuing bank (37 percent), the merchant (33 percent) and the card processor (15 percent).

Organizations that Suffered Financial Loss from Corporate Card Fraud in 2007
(Percentage Distribution of Organizations Subject to Corporate Card Fraud)

Organization suffered financial loss	33%
Organization did not suffer financial loss	67

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Other Parties that Assumed Liability for Financial Loss from Corporate Card Fraud in 2007
(Percentage Distribution of Organizations Subject to Corporate Card Fraud)

No other party assumed liability	22%
Card issuing bank	37
Merchant	33
Card processor	15
Other	22

B2B Card Fraud Control: Best Practices

With continued growth in the use of corporate cards—especially purchasing cards—for B2B payments, organizations have implemented a range of controls against fraudulent use of their cards. Controls have been put in place at various stages of card administration—at program set-up, as an ongoing procedure and as part of the management oversight function.

As an ongoing procedure, most organizations that use corporate cards:

- Require original receipts for purchases and/or print-outs of Web confirmations of purchases (78 percent).

When setting up the program, organizations:

- Define card spending limits by employee or by employee level; not the same for all employees (68 percent)
- Assign a permanent administrator to train cardholders and monitor usage (67 percent)
- Develop a detailed cardholder agreement that both cardholders and supervisors must sign (54 percent).

As an oversight procedure, however, less than half of organizations:

- Conduct a monthly management review of compliance with card usage policies and procedures (42 percent)
- Conduct surprise audits of compliance with card usage policies and procedures (34 percent).

Controls Adopted to Protect Against Fraudulent Use of Corporate Cards
(Percent of Organizations that use Corporate Cards to Make B2B Payments)

Require original receipts for purchases and/or print-outs of Web confirmations	78%
Define card spending limits by employee or by employee level	68
Assign a permanent administrator to train cardholders and monitor usage	67
Develop a detailed cardholder agreement that cardholders and supervisors must sign	54
Conduct a monthly management review of compliance with card usage policies and procedures.	42
Conduct surprise audits of compliance with card usage policies and procedures.	34
Design cards that look different from personal credit cards to minimize “accidental” use	29

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Commenting on the effectiveness of corporate controls in preventing or detecting payments fraud, organizations emphasized the importance of both internal oversight and vigilance against outside parties.

- *As a result of audit reviews on our corporate card, we were able to detect employee misuse.*
- *We have committed to a 100 % audit of all cardholder statements. The cardholders are aware of the audit policy and maintain usage within our policy guidelines.*
- *There are so many controls and reports built into the card programs that it makes it difficult not to detect fraudulent usage, provided you have an administrator monitoring the activity.*
- *It's mostly up to internal controls and auditing of card usage, and you still can't stop external parties from getting and using card numbers. All our fraud attempts have been from the outside.*
- *Company controls were sufficient to prevent internal abuse. But corporate card numbers were copied by an external party and used to make purchases. These purchases were flagged by the corporate card company and brought to our attention.*

Consumer Electronic Payments Fraud

Forty-three percent of respondents indicate that their organizations receive ACH and/or card payments from consumers. Of these, only ten percent indicate that they were victims of attempted or actual consumer ACH and/or card payments fraud in 2007.

Most fraud is committed by thieves using credit cards. Eighty-nine percent of organizations that were subject to consumer electronic payments fraud indicate that credit cards were used. More than one-third experienced ACH fraud and one-quarter reported signature debit card fraud. PIN debit cards were used much less frequently to commit fraud.

Electronic Payment Methods Subject to Consumer Payments Fraud
(Percent of Organizations Subject to ACH and/or Card Payments Fraud from Accepting Consumer Payments)

Credit cards	89%
ACH	38
Signature debit cards	24
PIN debit cards	11

Over one-third of organizations that were subject to consumer electronic payments fraud experienced more fraud in 2007 than they did in 2006. Most other organizations (61 percent) indicate there was little change from the previous year.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Change in Prevalence of Consumer Payments Fraud in 2007 Compared with 2006
(Percentage Distribution of Organizations Subject to Consumer ACH and/or Card Payments Fraud)

More fraud in 2007	37%
About the same	61
Less fraud in 2007	2

Two-thirds of organizations that were subject to ACH and/or card payments fraud suffered financial losses as a result. Organizations that accept electronic payments online were most likely to suffer financially. Seventy-one percent of organizations that had financial losses report that the loss originated from online commerce. Sixty-three percent experienced financial losses from in-person transactions, while 46 percent did so by accepting fraudulent ACH and/or card payments over the phone.

Channels Used to Commit Consumer ACH and/or Card Payments Fraud Resulting in Financial Loss
(Percent of Organizations Subject to Financial Loss Resulting from Consumer ACH and/or Card Payments Fraud)

Online via the Web	71%
In person (e.g., store or branch location)	63
Over the phone	46

Most organizations (92 percent) suffered financial loss from credit cards. Other payment methods used to commit consumer payments fraud were less likely to result in loss to organizations accepting that payment method.

- ACH (36 percent)
- Signature debit cards (28 percent)
- PIN debit cards (20 percent).

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Conclusion

Assaults against the payments system by criminals intent on committing fraud continued at full force in 2007. The prevalence of payments fraud and the varied methods by which it is carried out require the constant attention of treasury and finance professionals responsible for safeguarding their organizations' assets.

Almost three-quarters of respondents to the AFP survey report that their organizations were victims of payments fraud in 2007. Checks were the most vulnerable payment instrument. Almost all organizations (94 percent) that experienced attempted or actual payments fraud were victims of check fraud in 2007, a result relatively unchanged from 2006. Although check usage is declining nationwide, organizations that issue checks will continue to be exposed to check fraud.

Switching from checks to electronic payments can be a fraud-fighting tool. Organizations are much less likely to be subject to fraud from electronic payments than from checks. However, electronic payments require strong fraud defenses, too. Among organizations that were victims of attempted or actual payments fraud in 2007, 26 percent experienced ACH debit fraud and 13 percent experienced corporate card fraud. Large organizations with annual revenues over $1 billion—which are more likely to use electronic payments—were also more likely to have experienced an increase in fraud from ACH debits and corporate cards.

Organizations should be on guard against internal payments fraud, as well as fraud from external sources. Almost two out of five organizations that suffered financial losses from ACH fraud report that internal fraud (e.g., employee responsible) was the reason for the loss. Half of organizations that experienced corporate card fraud indicate that employees were responsible for at least some of the fraud.

Effective defense against payments fraud requires a range of fraud-fighting tools. Best practice organizations employ a two-pronged approach: 1) implementation of tight internal controls, and 2) use of banks' anti-fraud services.

The most effective check fraud services are positive pay/reverse positive pay and payee positive pay. They are used by best practice organizations in combination with internal controls such as daily reconciliation and separation of duties. Direct deposit of pay and payroll cards will reduce fraud associated with employee pay checks. Best practice organizations reinforce these electronic payment methods with ACH debit blocks and payee positive pay for the remaining checks.

To protect ACH payments from fraud, best practice organizations use ACH debit blocks and ACH debit filters. To prevent financial losses, they also reconcile their accounts daily and ensure that unauthorized ACH entries are returned on a timely basis.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

With continued growth in the use of corporate cards—especially purchasing cards—for B2B payments—organizations have instituted internal controls at various stages of card administration—at program set-up, as an ongoing procedure, and as part of the management oversight function. Constant vigilance is also required against external parties creating fraudulent corporate cards to make purchases. Organizations that experienced fraud from accepting ACH and/or card payments from consumers report that the majority of fraud was committed by thieves using credit cards; the least amount of fraud came from use of PIN debit cards.

Finally, online delivery processes used to send and receive electronic payments require their own set of internal controls and bank security services. Most organizations deploy a variety of internal controls to protect their online payments activity. Almost nine out of ten organizations, for example, segregate responsibilities among employees for payments template maintenance, payments entry and payments approval. A similar percentage use the multi-factor authentication tools offered by their banks, such as tokens, digital certificates and smart cards.

Gathering the forces to fight fraud requires a team approach. Accounts payable, audit, IT and human resources departments have joined with treasury to safeguard payment systems and keep defenses strong.

The battle against payments fraud will require innovative technical tools and high alert to guard against the new technical capabilities and practices of criminals. Fortunately, as this survey shows, many organizations are successfully fighting back.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

About the Respondents

On January 9, 2008, the Research Department of the Association for Financial Professionals (AFP) surveyed 3,950 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 488 responses yield an adjusted response rate of 14 percent. Additional surveys were sent to non-member corporate practitioners holding similar job titles and generated an additional 64 responses. The following tables provide a profile of the survey respondents.

Industry Classification
(Percentage Distribution)

Manufacturing	21%
Retail	11
Insurance	9
Energy	9
Government	8
Non-profit	7
Health services	7
Financial services	6
Real estate	5
Transportation	4
Telecommunications	4
Software/technology	3
Hospitality	3
Business services/consulting	3
Construction	2

Annual Revenues
(Percentage Distribution)

Under $50 million	5%
$50 – 99 million	4
$100 – 249.9 million	10
$250 - 499.9 million	12
$500 - 999.9 million	12
$1 – 4.9 billion	32
$5 – 9.9 billion	10
$10 – 19.9 billion	7
Over $20 billion	8

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

Ownership Type
(Percentage Distribution)

Publicly owned	47%
Privately held	32
Non-profit	11
Government	10

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)

	All Organizations	Revenues over $1 billion	Revenues under $1 billion
Checks	99%	99%	99%
Wire transfers	96	99	93
ACH credits	93	97	88
ACH debits	84	84	85
Corporate cards	73	80	64
Consumer ACH and/or card payments*	43	41	42
Prepaid/gift cards	11	12	8

* receive only

AFP thanks the Electronic Payments Network (EPN) for underwriting the 2008 Payments Fraud and Control Survey. Both questionnaire design and the final report were the responsibility of the AFP Research Department, which is solely responsible for the content and conclusions.

 ©2008 Association for Financial Professionals, Inc. All Rights Reserved

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.

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