



2011 AFP
Payments Fraud
and Control Survey
Report of Survey Results

Underwritten by
J.P.Morgan

2011 AFP
Payments Fraud
and Control Survey
Report of Survey Results

March 2011

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

As a leader in payments technology and solutions, J.P. Morgan is deeply committed to increasing awareness of payments fraud. Once again, we are extremely pleased to sponsor the 2011 AFP Payments Fraud and Control Survey.

The importance of objective information and trend monitoring in fighting payments fraud cannot be underestimated. This survey, the seventh annual, presents an important tracking tool for organizations and their banks, helping them understand their vulnerabilities as well as the effectiveness of certain technologies and practices in preventing fraud. Acting on the knowledge gained from this research and others in the marketplace is the real task.

Losses from payments fraud affect every sector of our economy. Financial institutions, retail merchants, corporations in all industry segments and consumers — we all pay the price, either directly or indirectly. Most important, fraud can undermine confidence in the payments system itself, inhibiting the growth of commerce in all of its forms.

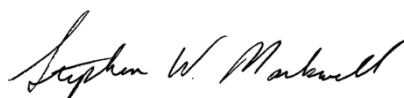
Despite advances in fraud protection and prevention in recent years, the rate of payments fraud attacks remains stubbornly high. The results of this year's survey show that, for the fifth consecutive year, seven of 10 organizations responding were victims of actual or attempted fraud.

While checks remain the overwhelming target, the steady migration from paper to electronic payment forms is moving fraud prevention to new focal points. ACH debits, corporate payment cards and Web-based access channels all present new frontiers. Organizations are also at increased risk due to the proliferation of mobile and other connected devices across the enterprise, the virtualization of business operations and the demographic shift toward online collaboration and social networking. These forces are dramatically changing the way business works, communicates, shares information and conducts transactions. And they underscore the need for new security models that acknowledge those changes.

Only with accurate and up-to-date knowledge of fraudster practices and the products and services available to combat them can organizations implement the internal procedures and external security services that will protect valuable assets. While the economic world becomes more complex, J.P. Morgan's technology, considerable experience and streamlined implementation processes make cutting-edge fraud protection simple to put in place and effortless to manage — protection that's automatic, effective, proven.

As we continue to invest in the technology, tools and expertise that companies need to prevent fraud attacks, J.P. Morgan provides accurate and up-to-date news and information and an arsenal of fraud-fighting tools that can help keep your organization safe from payments fraud.

With best regards,



Stephen W. Markwell
Executive Director

Introduction

If 2009 was the year of the “Great Recession,” perhaps 2010 was the year of the “Great Hangover.” While the economy and the U.S. financial system began to improve, the nation was still suffering from slow economic growth and high unemployment. In that environment, it was perhaps not surprising that companies maintained recession-inspired lean staffs. At the same time, continued economic challenges for many people presented criminals with opportunities for active threats, and fraud levels remained stubbornly high.

Each year since 2005, the Association for Financial Professionals (AFP) has examined the nature and frequency of fraudulent attacks on business-to-business payments and the industry tools that organizations use to control payments fraud. Continuing that research, in January 2011 AFP conducted its annual Payments and Fraud Control Survey to capture the payments fraud experiences of organizations during 2010. Results of that survey are reflected in this, the *2011 AFP Payments Fraud and Control Survey* report.

This year’s report shows that criminals continue to take advantage of a fertile environment in which they can commit payments fraud. A majority of organizations experienced attempted or actual payments fraud in 2010. The results of the survey also reinforce the need for organizations to implement and closely follow a plan to mitigate their risks for such fraud, including using appropriate services and procedures to minimize exposure to losses for their company and other parties in the payment system.

AFP thanks J.P. Morgan for underwriting the *2011 AFP Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of the AFP Research Department. Information on the survey methodology can be found at the end of this report.

Executive Summary

The key findings of the 2011 AFP Payments Fraud and Control Survey include:

- Seventy-one percent of organizations experienced attempted or actual payments fraud in 2010.
 - Large organizations were significantly more likely to have experienced payments fraud than were smaller ones. Eighty-two percent of organizations with annual revenues over \$1 billion were victims of payments fraud in 2010 compared with 58 percent of organizations with annual revenues under \$1 billion.
- Twenty-nine percent of survey respondents report that incidents of fraud increased in 2010 compared to 2009.
- Checks were the dominant payment form targeted by fraudsters, with 93 percent of affected organizations reporting that their checks had been targeted. The percentage of organizations affected by payments fraud via other payment methods were:
 - ACH debit (25 percent)
 - Consumer credit/debit cards (23 percent)
 - Corporate/commercial cards (15 percent)
 - ACH credits (four percent)
 - Wire transfers (four percent)
- Seventy-one percent of organizations that were victims of actual and/or attempted payments fraud in 2010 experienced no financial loss from payments fraud.
- Among organizations that did suffer a financial loss resulting from payments fraud in 2010, the typical loss was \$18,400.

Fraud Control

- Organizations turn to a number of fraud control services provided by their banks, including:
 - Positive pay/reverse positive pay (84 percent)
 - ACH debit blocks (76 percent)
 - ACH debit filters (61 percent)
 - Payee positive pay (58 percent)
 - “Post no checks” restriction on depository accounts (42 percent)
- The most prevalent reason why an organization does not use a particular fraud prevention service is cost/benefit does not justify its use (36 percent).
- Organizations develop and/or modify internal business processes to mitigate potential payments fraud risks. The processes considered important include:
 - Eighty-eight percent of organizations have increased their use of electronic payments for their business-to-business (B2B) transactions.
 - Eight-six percent of organizations have increased their use of electronic payments to employees.
 - Eighty percent of organizations that have increased their use of electronic payments for business-to-consumer transactions did so with fraud prevention in mind.
- Organizations also use separate accounts for different payment methods as a fraud control technique. For example,
 - Seventy-five percent of organizations have separate accounts for disbursement and collections.

- Forty-seven percent of organizations have separate bank accounts by payment type (e.g., vendor specific, tax, payroll, dividends).
- Thirty-six percent of organizations have separate accounts for receiving ACH debit payments.
- Fourteen percent of organizations were subject to a fraud attempt targeting user IDs and passwords.

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 (68 percent)
 - Alteration of payee names on checks issued by the organization (56 percent)
 - Alteration of dollar amount on checks issued (35 percent)
- Fourteen percent of organizations that were victims of at least one attempt of check fraud during 2010 suffered a financial loss resulting from check fraud.

ACH Fraud

- Twelve percent of organizations that were victims of ACH fraud during 2010 suffered a financial loss as a result of such fraud.
- Organizations that suffered a financial loss as a result of ACH fraud generally did so because they did not follow best practices and/or neglected to execute their own business rules as expeditiously as they should have, including: ACH return not being timely, a criminal takeover of the organization's online system, or not using ACH positive pay.

Business-to-Business Card Payments Fraud

- Seventy-seven percent of organizations that experienced payments fraud via the use of their own corporate/commercial cards report that an unknown external party committed the fraud.
- Ten percent of those organizations that experienced fraud via the use of their own corporate/commercial cards report that the fraud was committed by a third-party, such as a vendor, professional services provider or business trading partner.
- Thirty-two percent of organizations subject to fraud via use of their own corporate/commercial cards during 2010 suffered actual financial losses resulting from the fraud.
- Fourteen percent of organizations that accepted corporate/commercial cards from their business-to-business partners suffered a financial loss resulting from fraud using such cards.
- The typical organization that is subject to PCI compliance spends \$13,400 per year to maintain that compliance.

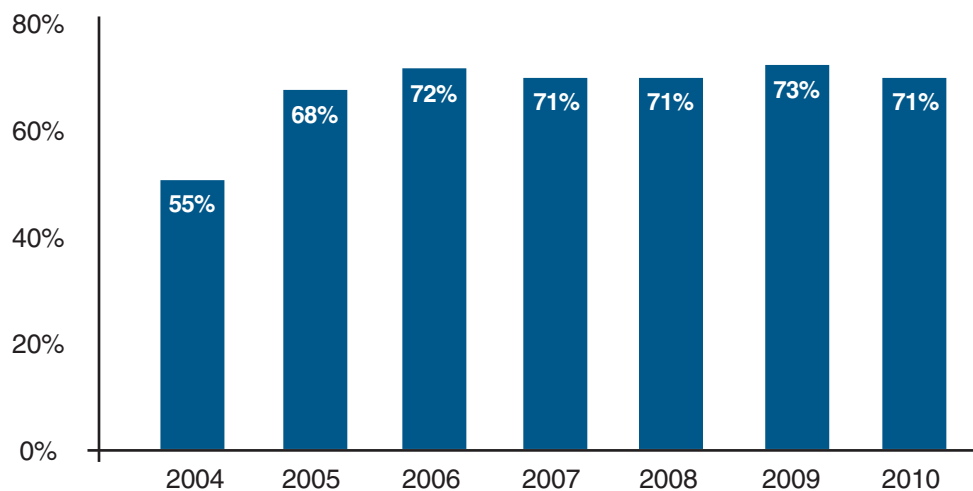
Survey Findings

Payments Fraud Overview

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. The need for that vigilance is apparent from the payments fraud experienced by organizations in 2010.

Fraud attacks on payment activities in 2010 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). Seventy-one percent of organizations experienced attempted or actual payments fraud in 2010. This was down two percentage points from 2009, but well within the tight range experienced over the past five years.

Percent of Organizations Subject to Attempted or Actual Payments Fraud



Large organizations were far more likely to have been the targets of payments fraud than were smaller ones. Eighty-two percent of organizations with annual revenues over \$1 billion were victims of payments fraud in 2010 compared to 58 percent of organizations with annual revenues under \$1 billion.

Organizations Subject to Attempted or Actual Payments Fraud in 2010
(Percentage Distribution)

	All Organizations	Revenues under \$1 billion	Revenues over \$1 billion
Organization was a victim of payments fraud	71%	58%	82%
Organization was not a victim of payments fraud	29	42	18

Checks remain the most popular target for criminals committing payments fraud. This is remarkable given the precipitous decline in corporate use of checks in recent years. Ninety-three percent of organizations that experienced attempted or actual payments fraud in 2010 were victims of check fraud, three percentage points above that reported in the 2009 survey. The second most popularly targeted payment types for fraud were:

- ACH debits (25 percent)
- Consumer credit/debit cards (23 percent)
- Corporate/commercial purchasing cards (15 percent).

Prevalence of Payments Fraud by Payment Method
(Percent of Organizations Subject to Attempted or Actual Payments Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Checks	93%	84%	95%
ACH debits	25	26	26
Consumer credit/debit cards	23	19	20
Corporate/commercial purchasing cards	15	19	18
ACH credits	4	*	11
Wire transfers	4	2	2

Twenty-nine percent of organizations report that the number of incidents of payments fraud attempts increased in 2010 compared to 2009. Nineteen percent indicate that the number of incidents declined, while the remaining 52 percent of respondents experienced no significant change in payments fraud activity in 2010 compared to 2009.

Change in Number of Attempted Payments Fraud in 2010 Compared to 2009
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Increased incidents of fraud	29%	28%	28%
About the same	52	49	56
Decreased incidents of fraud	19	23	16

Checks were the payment method most likely subject to an increased incidence of payments fraud, followed by consumer credit/debit cards and corporate cards. Thirty percent of survey respondents indicate that their organizations' checks were subject to a greater amount of payments fraud in 2010 than they were in 2009.

Payment Methods Subject to More Payments Fraud in 2010 Compared to 2009
(Percentage Distribution of Organizations Subject to Greater Amount of Attempted or Actual Payments Fraud in 2010)

	More	About the same	Less
Checks	30%	50%	20%
Consumer credit or debit cards	18	68	14
Corporate cards	16	69	15
ACH Debits	15	61	24
Wire Transfers	5	74	21
ACH Credits	3	74	23

Financial Loss from Fraud Attempts

Most payments fraud attempts involve relatively small amounts of money. For 53 percent of organizations that actually experienced payments fraud in 2010, the potential loss that could have resulted (or actually did result) from such fraud was less than \$25,000. For 28 percent of organizations, the potential loss was between \$25,000 and \$249,000, while the potential loss totaled at least \$250,000 for 19 percent of organizations.

The Potential Financial Loss Resulting from Attempted Payments Fraud in 2010
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Loss less than \$25,000	53%	58%	49%
Loss between \$25,000 and \$49,999	7	7	7
Loss between \$50,000 and \$99,999	11	16	10
Loss between \$100,000 and \$249,999	10	7	13
Loss greater than \$250,000	19	12	21
Median potential loss	\$23,500	\$21,000	\$28,600

Most organizations that were subject to at least one payments fraud attempt in 2010 did not suffer actual losses from the attempt. This is largely due to effective fraud detection and controls. Seventy-one percent of organizations experienced no financial loss from payments fraud, while another 19 percent realized a financial loss of less than \$25,000 during 2010. Among organizations that did suffer a financial loss resulting from payments fraud, the typical loss for the year was \$18,400. Large organizations sustained a median loss of \$20,600, 21.1 percent more than the median loss sustained by smaller organizations.

Actual Financial Losses from Attempted Payments Fraud in 2010
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
No loss	71%	70%	72%
Loss less than \$25,000	19	22	17
Loss between \$25,000 and \$49,999	3	4	2
Loss between \$50,000 and \$99,999	3	1	4
Loss between \$100,000 and \$249,999	1	*	1
Loss greater than \$250,000	3	3	4
Median actual loss#	\$18,400	\$17,000	\$20,600

- Of organizations that sustained financial losses resulting from payments fraud in 2010

For just over half of organizations, checks were the payment method through which the greatest percentage of financial loss resulted from payments fraud in 2010. Fifty-three percent of organizations that suffered financial loss resulting from payments fraud in 2010 suffered the greatest dollar loss from checks. The second most likely type of payments fraud resulting in the largest dollar loss was via consumer credit/debit cards (23 percent), while the third largest dollar loss was from fraudulent use of corporate cards (e.g., purchasing, T&E, fleet).

Payment Method Subject to the Greatest Financial Loss Resulting from Fraud in 2010
(Percentage Distribution of Organizations that Suffered Financial Loss from Payments Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Checks	53%	46%	55%
Consumer credit/debit cards	23	21	22
Corporate/commercial purchasing cards	14	18	15
ACH debits	8	11	8
ACH credits	1	4	*
Wire transfers	1	*	*

For most organizations that were subject to attempted and/or actual payments fraud in 2010, the cost to manage, defend and/or clean up from payments fraud events was, at most, relatively modest. Nearly two out of five organizations that were subject to at least one payments fraud attempt in 2010 did not expend any costs to defend against or clean up from the attempt. Fifty-two percent of organizations spent less than \$25,000 in 2010.

Costs Spent to Manage, Defend and/or Clean Up Payments Fraud Events in 2010
(Percentage Distribution of Organizations Subject to Attempted or Actual Payments Fraud)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
No loss	38%	44%	37%
Loss less than \$25,000	52	49	52
Loss between \$25,000 and \$49,000	4	3	6
Loss between \$50,000 and \$99,999	2	1	2
Loss between \$100,000 and \$249,999	1	*	1
Loss greater than \$250,000	3	3	2

Most payments fraud is the result of an action taken by an individual who is not a part of the victimized organization. Eighty-seven percent of organizations that suffered a financial loss resulting from payments fraud in 2010 did so as a result of actions taken by an outside individual (perhaps in the form of a forged check or a stolen credit/debit card). Ten percent of organizations were subject to payments fraud originating from an organized crime ring or from a third-party/outsourcer. Nine percent of organizations were subject to internal payments fraud.

Source of Payments Fraud that Resulted in Financial Loss in 2010
(Percent of Organizations that Suffered Financial Loss from Payments Fraud)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Outside individual (e.g., forged check, stolen card)	87%	86%	89%
Third-party or outsourcer (i.e., vendor, professional services provider, business trading partner)	10	11	7
Organized crime ring (e.g., city specific crime spree)	10	10	11
Internal party (i.e., malicious insider)	9	7	10
Other	5	2	5
Criminal invasion (i.e., hacked system, malicious code-spyware or malware)	3	1	4
Lost or stolen laptop or other device	*	1	*

Fraud Control

Organizations use a number of fraud control services offered by their financial institutions to protect their bank accounts. The most widely used fraud control measures used to guard against fraudulent checks are positive pay and/or reverse positive pay; these fraud controls compare a company's record of checks issued with checks presented for payment. Eighty-four percent of organizations use positive pay and/or reverse positive pay, including 87 percent of organizations with annual revenues greater than \$1 billion. Nearly three out of five organizations (regardless of size) also protect against check fraud by using payee positive pay to prevent the alteration of a payee name on checks. Forty-two percent of organizations place a "post no checks" restriction on depository accounts. Large organizations are significantly more likely to use check-related fraud control measures than are smaller organizations.

Organizations continue to increase their use of controls that protect against ACH fraud. Seventy-six organizations use ACH debit blocks to prevent unauthorized ACH transactions while 61 percent use ACH debit filters for pre-authorized ACH debits from known trading partners. The use of both of these ACH fraud control measures is more frequent among large organizations. Twenty-seven percent

of organizations use ACH positive pay while seven percent use Universal Payment Identification Code (UPIC), which can be used to mask sensitive bank account information for ACH credits.

Organizations have other, more general, fraud control services and methods at their disposal. Seventy-eight percent of organizations rely on daily reconciliation and other internal processes to prevent financial loss resulting from payments fraud. Nine percent also use non-bank fraud control services.

Respondents report slightly increased usage of several payment fraud control services and methods compared to that in the 2010 survey. They include:

- Payee positive pay
- “Post no checks” restriction on depository accounts
- ACH positive pay

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

		All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Checks	Positive pay/Reverse positive pay	84%	82%	87%
	Payee positive pay	58	51	65
	“Post no checks” restriction on depository accounts	42	33	49
ACH	ACH debit blocks	76%	65%	88%
	ACH debit filters	61	55	66
	ACH positive pay	27	27	26
	Universal Payment Identification Code for ACH credits	7	7	8
Other	Daily reconciliation and other internal services	78%	78%	76%
	Non-bank fraud control services	9	7	10
	Other	1	1	1

While most organizations use positive pay and ACH debit blocks and/or filters to prevent payments fraud, they may decide not to use one of these services for a variety of reasons. The most widely cited reason is cost benefit: 36 percent of organizations that do not use positive pay, debit blocks or UPIC choose to not to do so because they do not believe the benefits outweigh the costs of using the service(s).

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

	All Respondents
Cost/benefit does not justify using the services	36%
My organization uses another service to control the fraud	18
Service(s) is difficult to use or requires too much of my time	9
Daily large item review	9
My company does not issue enough checks/payments to justify use of the service(s)	9
Other (please specify)	27

In addition to purchasing fraud control services from their bank, many organizations develop their own internal measures and modify business processes to mitigate risk of payments fraud. Eighty-eight percent of organizations that have increased their use of electronic payments for their business-to-business (B2B) transactions, 86 percent that have increased use of electronic payments to employees, and 80 percent that have increased their use of electronic payments for business-to-consumer transactions did so with fraud prevention in mind. Four out of five organizations that have restricted their online data communications indicate that the desire to reduce payments fraud played an important role in the decision to do so. Seventy-seven percent of organizations report that fraud prevention was at least a “somewhat” important consideration when they decided to stop providing payment instructions by phone or fax.

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

	Important	Somewhat Important	Not at all Important
Increased use of electronic payments to employees (e.g., payroll cards, stored value cards, direct deposits to employee accounts)	52%	34%	14%
Increased use of electronic payments for B2B transactions	51	38	11
Restricted the use of online data communication	49	31	20
Increased use of electronic payments for non-payroll B2C transactions	45	35	20
Stopped giving payment instructions by phone or fax	44	33	23
Reduced the number of bank accounts	40	33	28
Did not provide my bank account number to payors for electronic payments	33	39	29
Outsourced accounts payable	16	28	56

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

Seventy-five percent of organizations maintain separate accounts for different payment methods and types. Of those organizations:

- Three-quarters have separate accounts for disbursement and collections
- Just under half separate accounts by payment type
- Thirty-six percent maintain separate accounts for wire transfers
- A third have separate accounts for receiving ACH debit payments

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 under \$1 billion	Revenues over \$1 billion
Separate accounts to segregate disbursements from collections	75%	68%	80%
Separate accounts by payment type (e.g., to segregate vendor, tax, payroll, dividend)	47	44	45
Separate account for wire transfers	36	29	38
Separate accounts for receiving ACH debit payments	32	26	35
Separate account for card payments	24	21	24
Other (please specify)	3	*	2

Media attention has been focused on payment fraud attacks that targeted compromised user ID/ passwords and other security credentials to gain access to company accounts to execute payments fraud. In 2010, 14 percent of organizations were subject to a payments fraud attack involving compromised user IDs/passwords. Most organizations that were attacked did not have their systems or credentials compromised as a result.

Prevalence of Payments Fraud Attempt Targeting Compromised User IDs/Passwords in 2010
(Percentage Distribution)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Organization was not attacked using compromised user IDs/passwords	86%	87%	86%
Organization was attacked, but no systems or credentials were compromised	12	12	10
Organization was attacked and some systems or credentials were compromised	2	1	4

The vast majority of organizations that were subject to a payments fraud attempt targeting the organizations' user IDs and passwords reviewed and strengthened their internal procedures and controls as a result (79 percent). Just under half of attacked organizations adopted stronger forms of authentication or added layers of security.

Organizations' Response to Attack Resulting in Compromise of User IDs/Passwords
(Percent of Organizations Subject to an Attack Involving User IDs/Passwords)

Reviewed and strengthened internal procedures and controls	79%
Adopted a stronger form of authentication or added layers of security (e.g., adding out-of-brand authentication)	46
Started performing daily reconciliations	14
Replaced proprietary bank connections with secure access through the SWIFT network	5
Dedicated a PC (with no links to e-mail/web browsing) for payment origination	5
Other	5

Check Fraud

The typical organization that was subject to attempted/actual check fraud in 2010 faced a median of seven fraud attempts during the year. Forty-seven percent of organizations were subject to between one and five check fraud events while 14 percent experienced between six and ten events. Twenty-seven percent of organizations experienced a far greater number of check fraud events—at least 20. Large organizations were typically subject to two more check fraud events than were smaller organizations—seven versus five events.

Frequency of Attempted or Actual Check Fraud in 2010
(Percentage Distribution of Organizations Subject to At Least One Attempt of Check Fraud in 2010)

Number of Attempts	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
1-5	47%	55%	44%
6-10	14	15	13
11-15	7	3	8
16-20	7	6	7
20 or more	25	21	28

Sixty-eight percent of organizations that were subject to check fraud in 2010 indicate that the fraud was perpetrated through the use of counterfeit checks using the organization’s MICR line data. Fifty-six percent of organizations that were subject to check fraud in 2010 report that the criminals altered payee names on checks issued by the organization, while 35 percent of organizations report that check fraud resulted from alteration of the dollar amount on checks they had issued.

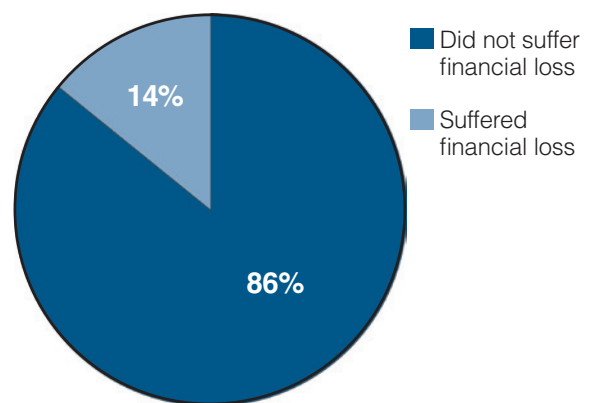
Types of Fraud Resulting from Using Checks
(Percent of Organizations that Suffered Check Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Counterfeit checks (other than payroll) using organization’s MICR line data	68%	64%	71%
Payee name alteration on checks issued	56	50	59
Dollar amount alteration on checks issued	35	34	35
Counterfeit check with your name drawn on fake or another company’s account information	28	27	28
Loss, theft or counterfeit of employee pay checks	19	13	21
Other	4	8	3

Even if check fraud is the prevalent type of fraud, most organizations do not suffer financial losses as a result. Fourteen percent of organizations that suffered check fraud in 2010 incurred financial loss from the check fraud. Large organizations were slightly more likely to have suffered financial loss resulting from check fraud in 2010 than were smaller organizations (15 percent versus nine percent).

Check Fraud Resulting in Financial Loss

Organizations that did suffer a financial loss resulting from check fraud identify a number of factors that led to the loss. Nearly half of organizations that suffered a financial loss resulting from check fraud report that the check used in the fraud was cashed by a check-cashing service. A third of organizations that suffered financial loss from check fraud tied the loss to not reconciling accounts/reviewing positive pay on a timely basis, while internal fraud was the cause for financial loss at 29 percent of organizations.



Cause of Loss Due to Check Fraud
(Percent of Organizations that Suffered a Loss Resulting from Check Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Loss due to check cashed by check-cashing service	46%	43%	45%
Loss due to account reconciliation or positive pay review not timely	32	14	40
Loss due to internal fraud (e.g., employee responsible)	29	29	25
Loss due to untimely check return	14	0	20
Other	14	29	10
Loss due to not using positive pay, reverse positive pay or payee positive pay	7	14	5
Loss due to not using "post no checks" service on electronic payment account	7	0	10

Once an organization is a victim of check fraud, the top concern for 37 percent of organizations is recovering the stolen funds. For a third of respondents, the organizations' top concern after detecting check fraud is working with law enforcement on the identification and prosecution of the criminals.

Organizations' Top Concern as a Result of Check Fraud
(Percentage Distribution of Organizations that Suffered a Loss Resulting from Check Fraud in 2010)

Recovering the stolen funds	37%
Working with law enforcement to identify and prosecute fraudsters	33
Preserving ability for employees to cash checks	15
Managing negative impacts to your organization's reputation in local communities	11
Other	4

While 56 percent of responding organizations convert checks for transmission to their banks as electronic items, virtually none of these organizations have suffered fraud using the check conversion service. Just one percent of organizations that convert checks electronically indicate that the check conversion service was used to commit fraud.

Electronic Check Conversion Service Used as a Vehicle to Commit Fraud
(Percentage Distribution of Organizations that Electronically Convert Checks)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Organization's electronic check conversion service was used to commit fraud	1%	*	1%
Organization's electronic check conversion service was not used to commit fraud	99	99	99

ACH Fraud

Not only does ACH fraud affect a relatively small number of organizations, it occurs rather infrequently even among those organizations that have been affected by it. Among organizations that were a victim of attempted and/or actual ACH fraud in 2010, the typical organization was subject to four ACH fraud attempts during the year.

Frequency of Attempted or Actual ACH Fraud in 2010
(Percentage Distribution of Organizations that Suffered ACH Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
1-5	65%	71%	63%
6-10	16	14	15
11-15	8	10	7
16-20	3	5	3
20 or more	8	*	12
Median # of incidents	4	4	4

Only 12 percent of organizations that were subject to at least one ACH fraud attempt in 2010 suffered a financial loss as a result. Smaller organizations were only slightly more likely to have suffered financial loss as a result of ACH fraud in 2010 than were organizations with annual revenues greater than \$1 billion.

The most likely reasons why the organization was financial responsible for the losses sustained from the ACH fraud include:

- Not reconciling accounts on a timely basis
- Not using ACH debit blocks or ACH debit filters
- ACH return not being timely
- Not using ACH positive pay.

ACH Fraud Resulting in Financial Loss
(Percentage Distribution of Organizations that Suffered ACH Fraud in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Did not result in financial loss	88%	86%	90%
Resulted in financial loss	12	14	10

Most organizations do not have difficulty in meeting the 24-hour deadline for returning ACH debits. Fifty-nine percent of organizations that were subject to ACH fraud in 2010 indicate that they do not have any difficulty in meeting the 24-hour deadline for returning ACH debits. Another 11 percent of organizations “rarely” have difficulty in meeting the deadline while a quarter indicate that they sometimes have difficulty.

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

Organization does not have difficulty meeting the deadline	59%
Organizations rarely has difficulty meeting the deadline	11
Organization sometimes has difficulty meeting the deadline	27
Organization regularly has difficulty meeting the deadline	3

There are a variety of actions that an organization can take in order to meet the 24-hour deadline for returning ACH debits. Fifty-five percent of organizations return ACH debits if they cannot easily identify the originator of the debit. Seventeen percent of organizations have identified the best practices that their peers use to manage the process while 12 percent provide a customer service number from the originator.

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

Not a problem--organization returns ACH debits if the originator cannot be readily identified	55%
Identify best practices companies use to manage this process	17
Provide a customer service number from the originator	12
Ensure the company name is readily recognized	9
Other	7

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

Seventy-six percent of respondents indicate that their organizations use corporate/commercial cards for business-to-business (B2B) payments. Purchasing cards are the most likely used forms of corporate/commercial cards (73 percent), followed by travel and entertainment (T&E) cards (44 percent), ghost or virtual cards (32 percent) and cards that combine many uses (29 percent).

Types of Cards Used in Making B2B Payments (Percent of Organizations Subject to Card Fraud in 2010)

Purchasing Cards	73%
T&E cards	44
Ghost or virtual cards	32
“One card” combining many uses	29
Fleet Cards	13
Airline travel cards (UATP)	6

Nearly half of organizations that suffered fraud associated with corporate/commercial cards in 2010 report that they did so through the use of their own corporate/commercial cards. Smaller organizations were more likely than large organizations to have suffered fraudulent activity on their corporate/commercial cards in 2010.

Fraud Resulting from Organizations’ own Corporate/Commercial Card Payments (Percentage Distribution of Organizations that Experienced Fraud Associated with Corporate/Commercial Cards in 2010)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Experienced Fraud	48%	64%	36%
Did not Experience Fraud	52	36	64

Typically, payments fraud involving an organization’s own corporate/commercial cards is committed by an outside party. More than three quarters of organizations that were subject to fraud via their own corporate/commercial cards indicate that the fraud was perpetrated by an unknown external party (77 percent). Only ten percent of such organizations report that the fraud was committed by a known third-party, such as a vendor, professional services provider or business trading partner. Despite the prevalence of corporate/commercial card fraud by outside parties, a significant amount of such fraud is committed by an organization’s own employees. Just over a quarter of organizations were subject to fraud by their own employees using the organizations’ corporate/commercial cards (29 percent).

Primary Party Responsible for Fraud from Making B2B Card Payments

(Percent of Organizations that Suffered Attempted or Actual Fraud Using Organizations' Corporate/Commercial Cards in 2010)

External	Unknown external party	77%
	Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	10
Internal	Employee	29

When an organization's own checks were used to perpetrate fraud, those incidents frequently did not result in financial liability to the organization. But this is not typically true in cases involving corporate/commercial cards. A third of organizations that were subject to corporate/commercial card fraud during 2010 suffered actual financial losses. Other parties that suffered financial loss as a result of corporate/commercial card fraud include the bank or financial institution that issued the card (45 percent) and the merchant where the card was used (32 percent).

When an organization is responsible for the financial loss associated with fraudulent use of its corporate/commercial cards, it is usually because of employee loss.

Organizations Suffering Loss as a Result of B2B Corporate/Commercial Cards Fraud

(Percent of Organizations that Suffered Attempted or Actual Fraud Using Organizations' Corporate/Commercial Cards in 2010)

Card issuing bank	45%
The organization	32
Merchant	32
Other	13
No organization suffered financial loss	6
Card processor	6

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

Only 14 percent of organizations that accept corporate/commercial cards from their business-to-business partners suffered a financial loss resulting from fraudulent use of such cards.

Financial Loss Due to Accepting Corporate/Commercial Cards in 2010

(Percentage Distribution of Organizations that Experienced Fraud Associated with Accepting Corporate/Commercial Cards)

Experienced financial loss	14%
Did not experience financial loss	86

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

- It is a card-not-present merchant that usually assumes liability
- Organization did not authenticate the cardholder
- Organization delayed its chargeback response.

PCI Compliance

PCI refers to the PCI Data Security Standard and the compliance programs that the card networks and acquirers mandate for merchants that accept cards. PCI sets the standard for the security measures merchants must implement to protect static card account numbers and other sensitive information. The standard is intended to provide an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents.

The typical organization that is subject to PCI compliance spends \$13,400 per year to maintain that compliance. Large organizations spend more than twice what smaller organizations spend to maintain PCI compliance (\$20,400 versus \$9,100 per year).

Organizations' Cost for Compliance to the PCI Digital Security Standard (Percentage Distribution of Organizations Subject to PCI Digital Security Standards)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Less than \$10,000	45%	55%	34%
\$10,000-\$25,000	22	21	23
\$25,001-\$50,000	12	12	12
\$50,001-\$100,000	6	5	7
\$100,001 or greater	15	7	23
Median expense	\$13,400	\$9,100	\$20,400

Conclusions

The Great Recession and Great Hangover in the U.S. have done little to help reduce payments fraud. However, this and prior AFP payments fraud surveys show the level of fraud activity has been consistent over the past several years. Nevertheless, with over 70 percent of companies hit by attempted or actual losses in 2010, fraud remains persistently high.

Despite the precipitous drop in check volume over the last several years, checks continue to be widely used and abused, and fraud via check payments remains the overwhelming threat faced by companies. Ninety-three percent of the fraud attempts and 53 percent of the actual losses incurred by companies from payments fraud are from some type of check fraud. Organizations also remain vulnerable from consumer and/or corporate/commercial card fraud due to the ease with which criminals can exploit the card networks, with consumer cards (16 percent of organizations citing such fraud) not surprisingly proving more vulnerable to fraud than commercial cards (cited by 11 percent of organizations). Payments via ACH and wires are relatively secure, but over 14 percent of respondents were hit by hackers trying to gain access and take over their corporate accounts—so even these networks can be exploited for fraud.

Given recent history, two fundamental questions emerge: (1) why is fraud so rampant and (2) can organizations do more to minimize risk and actual losses? The answer to the first question is obvious: the cost/benefit equation for criminals is still positive—many are rewarded handsomely for the level of risk they take. The second question is more complex. While there will prob-

ably always be more that corporations can do to minimize fraud, they also need to examine their own cost/benefit equation—including how much time they must invest every day to deal with fraud risks.

The Cost/Benefit Equation – Criminals

The majority of fraud occurs via three payment types: checks, consumer cards and commercial cards. Fraud is very limited with ACH and wires (and check conversion). The primary difference is obvious—the first three payment methods provide opportunities for individuals and third parties to gain easy access to static account information via the payment process. Outside individuals were responsible for check fraud losses 87 percent of the time. For B2B card payments an unknown external party was responsible for fraud attempts or losses 77 percent of the time. Essentially all hackers attacking organizations remotely are unknown third parties.

With broad access and remote channels through which they can commit fraud, criminals are naturally drawn to the inherent insecurity of the check and card payment systems. Corporates, banks, networks, and other processors do their best to monitor, detect and prevent fraud attacks, but it is a monumental challenge. Criminals continue to be successful. Losses from check fraud occur most frequently (53 percent) compared to those from other payment methods, and the magnitude of those losses continue to climb—up eight percent over last year to an average of \$18,400. Unless the cost/benefit equation changes dramatically, we can expect criminals to continue their frequent attacks on corporates and other participants in the payments system.

The Cost/Benefit Equation – Corporates

The Treasury and payment systems of organizations are attacked for the most obvious reason—that’s where the money is. As a result, companies are forced to invest significant time and money to avoid losses and minimize the impact of any fraud attempts, including paying for bank services, establishing internal procedures and controls, and dealing with all of the exceptions that continually arise from errors, omissions and actual fraud attempts.

The nature of these attacks is very broad, which adds to the heavy burden corporates must bear. Fourteen percent of organizations report their payment systems were “hacked” in 2010 (two percent report their systems were compromised) and that percentage appears to be growing rapidly. Only four percent of corporates reported “criminal invasions” in 2009. The use of cards comes with the special burden of PCI compliance (at an average cost of \$13,400/year, with the cost escalating based on size of organization), and the managing of card acceptance policies and controls for company-controlled commercial cards.

Still, the most well-established and active fraud attacks are via checks: 68 percent of corporates experienced counterfeits, 56 percent had payee name alterations, and 35 percent encountered amount alterations. Furthermore, 25 percent of organizations had 20 or more check fraud attempts in 2010—basically one every other week.

Companies feel a special sense of urgency about fraud associated with payroll checks. Payroll checks are a major source of checks used to commit fraud (cited by 19 percent of organizations). Losses result-

ing from holder in due course situations, primarily related to duplicate checks negotiated at check-cashers are escalating rapidly. Forty-six percent of corporates cited this as the cause of loss, up from 37 percent in the 2009 survey.

Laws related to holder in due course are the foundation for check acceptance in the U.S., so corporates have limited options when encountering these situations. As a result, in spite of antiquated laws in some states that prevent employees from adopting electronic payments in greater numbers, many companies (86 percent in the survey) continue to mount major efforts to convert all of their payroll checks to direct deposit or payroll cards—with options to deliver pay stubs electronically.

Corporates use many strategies to cope with their fraud burden:

Checks

- Many organizations are simply moving away from checks. They recognize that most of the float has been squeezed out of the check-clearing process, making it more cost-effective to focus on the other benefits from electronic payments—liquidity visibility, greater automation and cost savings, as well as the obvious fraud control benefits
- Companies continue to use fraud services and internal controls to detect fraud and for time-management purposes. Positive pay, reverse positive pay and payee positive pay are still relied upon by well over half of corporates. Daily reconciliation is also used by many companies (78 percent), particularly on high-dollar or other sensitive accounts.
- Companies have also developed other anti-

fraud strategies. Many organizations will segregate accounts by purpose and then add specific account controls. For example, electronic payments may be directed to one or more accounts that have a “post no checks” order to prevent fraud and eliminate the time corporates must spend reviewing rejected items.

ACH

- One reason companies like to use ACH is because the processing cost is typically less than that for checks or wires. ACH is also much easier to control. For example, many companies segregate their ACH debit payments to a separate account and apply an ACH debit filter or ACH positive pay service on the account. For non-ACH debit accounts, debit blocks are deployed. If implemented properly, organizations eliminate or minimize the number of items they must review to identify fraudulent items.
- The UPIC continues to be underutilized by companies, but this effective fraud control tool should be considered by all companies as a way to enable the company to freely share account numbers (the UPIC) on invoices they send to customers from whom they want to receive ACH credits.

Cards

- Corporates do have some tools, like spending controls, to help minimize fraud on commercial cards. However, both consumer and commercial cards depend on static account information that can be skimmed from a card or stolen from a database. Once the account information is compromised, it is relatively easy to perpetrate fraud. Rather than continuing to dump money

into PCI compliance programs geared toward protecting static account numbers, the results from this survey suggest that it is time to upgrade the card networks to reflect the current environment. Otherwise organizations will continue to face significant losses when cards are compromised.

Eliminating checks continues to be the single best way for organizations to combat fraud. The card networks are more secure than checks, but card fraud attempts and losses from such fraud continue to occur at high rates. (They only seem low when compared to the incidence of check fraud.) Corporates must remain vigilant in monitoring their accounts against fraud and make the best choices they can when choosing to accept or make payments with checks and cards. They must also adopt best practices against hackers and corporate account takeover situations—the instances of fraud are growing in this area and appropriate precautions must be taken.

Finally, corporates need to decide if they are collectively doing enough to demand secure payment services—finding ways that minimize disruption to their internal payment operations, support full automation/STP, and are provided at a reasonable cost. Corporates also need to make sure they do their part to support the industry in developing and sustaining initiatives that work to each organization’s ultimate benefit. That support includes offering guidance to their banks and other vendors as well as by providing direct input and leadership on payments industry initiatives.

About the Respondents

In January 2011, the Research Department of the Association for Financial Professionals (AFP) surveyed 5,200 of its corporate practitioner members about payments fraud and controls. The survey was sent to AFP corporate practitioner members with the following job titles: cash managers, analysts, and directors. After eliminating surveys sent to invalid and/or blocked email addresses, the 337 responses yielded an adjusted response rate of eight percent. Additional surveys were sent to non-member corporate practitioners holding similar job titles and generated an additional 62 responses. The following tables provide a profile of the survey respondents.

AFP thanks J.P. Morgan for underwriting the *2011 Payments Fraud and Control Survey*. Both questionnaire design and the final report, along with its content and conclusions, are the sole responsibility of the AFP Research Department.

The following tables provide a profile of the survey respondents, including payment types used and accepted.

Industry Classification (Percentage Distribution)

Manufacturing	19%
Retail (including wholesale/distribution)	13
Government	11
Energy (including utilities)	9
Health services	9
Banking/Financial services	7
Insurance	6
Non-profit (including education)	6
Real estate	5
Telecommunications/Media	5
Business services/Consulting	3
Software/Technology	3
Transportation	2
Construction	1
Hospitality/Travel	1

Annual Revenues (Percentage Distribution)

Under \$50 million	6%
\$50-99.9 million	3
\$100-249.9 million	10
\$250-499.9 million	10
\$500-999.9 million	17
\$1-4.9 billion	31
\$5-9.9 billion	9
\$10-20 billion	7
Over \$20 billion	7

Organization's Ownership Type (Percentage Distribution)

Publicly owned	40%
Privately held	37
Non-profit (non-for-profit)	12
Government (or government owned entity)	11

Payment Methods Used by Organizations to Make Payments
(Percent of Organizations)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Checks	98%	99%	99%
Wire transfers	95	95	98
ACH debits	79	82	80
ACH credits	78	73	85
Corporate/commercial purchasing cards	76	72	82
Consumer credit/debit cards	23	22	25

Payments Methods Used to Pay Organizations
(Percent of Organizations)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
Checks	94%	93%	97%
ACH credits	90	88	93
Wire transfers	88	85	93
ACH debits	58	54	61
Consumer credit/debit cards	57	59	56
Corporate/commercial purchasing cards	40	38	43

Organizations' Volume of Payments Transactions
(Percentage Distribution)

	All Respondents			Revenues under \$1 billion			Revenues over \$1 billion		
	Consumers	Split	Business	Consumers	Split	Business	Consumers	Split	Business
Making Payments	3%	23%	74%	3%	18%	79%	5%	25%	70%
Receiving Payments	20	34	46	21	29	50	20	36	44

Prevalence of Check Conversion for Transmission to the Bank as Electronic Items
(Percentage Distribution)

	All Respondents	Revenues under \$1 billion	Revenues over \$1 billion
No	44%	50%	40%
Yes, check images	36	35	37
Yes, both ACH and check image	14	8	17
Yes, via ACH	6	7	6

AFP Research

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



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

WHAT MATTERS TODAY

Efficiency

An efficient treasury operation is instrumental to a healthy, growing company. Whether the need is to rationalize global account structures, streamline payables, or unlock working capital across the supply chain, the trusted advisors of J.P. Morgan can help.

Our clients benefit from our global reach, local experience and flexible treasury product solutions – all supported by outstanding service and market-leading technology.

- CASH MANAGEMENT
- TRADE
- LIQUIDITY
- COMMERCIAL CARD
- ESCROW SERVICES



TO DISCUSS HOW TO MAKE YOUR TREASURY MORE EFFICIENT, call your J.P. Morgan treasury advisor, or find ideas online at jpmorgan.com/WhatMattersToday

J.P.Morgan