
Payments Risk Survey

Report of Survey Results

March 2006



Association for Financial Professionals
7315 Wisconsin Avenue, Suite 600 West, Bethesda, MD 20814
301.907.2862 Fax 301.907.2864 www.AFPonline.org

Payments Risk Survey

Introduction

Organizations today are engaged in a variety of initiatives to strengthen payments risk controls and protect the security, integrity and continuity of financial transactions. They are building defenses against fraud, tightening internal controls over the payments process and testing disaster recovery plans.

AFP conducted a survey in February 2006 to highlight ways that treasury and finance professionals are managing two categories of risk: fraud risk and operating risk. To examine the incidence of fraud and the effectiveness of fraud controls, the survey asked about actual and attempted efforts to divert funds from the organization, whether or not the organization suffered financial losses.

Operating risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people or systems associated with payment execution. To explore defenses against operating risk, the AFP survey included questions about an organization's internal controls over payments processes and its plans to continue making and receiving payments in the event of a natural disaster or systems failure.

The responses to the survey spotlight best practices for mitigating payments risk and can help to increase awareness of actions that payment system participants can take within their organizations and in cooperation with their service providers to prepare for the unexpected.

Highlights of Survey Results

Key findings of the Payments Risk Survey include:

Payments Fraud

- Sixty-eight percent of organizations were targets of attempted or actual payments fraud in 2005.
 - Seventy-nine percent of organizations with annual revenues greater than \$1 billion report payments fraud in 2005, compared to 54 percent of organizations with annual revenues below \$1 billion.
 - The prevalence of payments fraud in 2005 was largely unchanged from 2004, with fifty-five percent of organizations reporting that incidents of fraud remained about the same in 2005 as in 2004.
 - Large organizations are more likely to experience an increase in payments fraud than smaller organizations.
- Checks and ACH debits were the most frequently used vehicles for payments fraud.
 - The majority of organizations did not suffer a financial loss as the result of check and ACH debit fraud.

- Positive pay or reverse positive pay was the fraud control measure most responsible for preventing financial losses from check fraud.
- Twenty-seven percent of organizations that reported an incident of ACH debit fraud lost money as opposed to 19 percent of the victims of check fraud.
- ACH debit blocks were the measure most responsible for preventing loss by victims of ACH debit fraud, with daily reconciliation or monitoring of balances and transactions cited by almost as many respondents.
- The majority of organizations (54 percent) that experienced card payments fraud suffered a financial loss.
 - Fifty-nine percent of organizations that suffered financial losses from card payments fraud were “card-not-present” merchants.

Internal Controls

- Nearly nine out of ten organizations (88 percent) have a written payments policy.
 - Only 38 percent of organizations update their policies on an annual basis.
 - Most written payments policies provide for separation of duties. They identify the departments that are authorized to request the payment, authorize the payment and execute the payment.
- Fifty-four percent of organizations made material changes to their payments controls as a result of Sarbanes-Oxley
 - Forty-six percent made no change; they are more likely to be organizations with annual revenues under \$1 billion.
 - Organizations that strengthened payments controls as a result of Sarbanes Oxley perform more frequent audits (28 percent), require additional approvals (26 percent), or require additional documentation related to the payment request (20 percent).
- To ensure compliance with payments control practices, 53 percent of organizations report that internal and/or external auditors perform surprise audits.

Disaster Recovery

- In 2005, one-quarter of organizations experienced a natural disaster or power or phone outage, while eighteen percent were impacted by a hardware or software failure.
- One-quarter of organizations do not have written disaster recovery plans.
- Large organizations are more likely to have written plans (81 percent) than smaller organizations (67 percent).
- Fifty-seven percent of organizations with disaster recovery plans test them at least annually; more than a third test only infrequently.
- Fifty-eight percent of organizations have designated back-up personnel to initiate and execute payments if regular staff is not available.
 - Less than half of organizations (44 percent) have authorization and approval procedures specifically for employees working off-site or at home.
- Only 45 percent of organizations indicate that their banks have communicated their disaster recovery plans for processing payments in the event of a disaster at the bank.
 - Three out of five organizations (59 percent) are either satisfied or very satisfied with their banks’ disaster recovery plans.

Survey Findings

Payments Fraud

Payments fraud in 2005 was widespread and broad-based, affecting organizations both large and small and showing no signs of letting up. Over two-thirds of organizations were targets of attempted or actual payments fraud last year.

Organizations with annual revenues over \$1 billion were much more likely than smaller organizations to be the victims of attempted or actual fraud. Seventy-nine percent of large organizations report payments fraud in 2005, compared to 54 percent of smaller organizations.

Prevalence of Payments Fraud in 2005

(Percentage of Respondents)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization was a victim of payments fraud	68%	79%	54%
Organization was not a victim of payments fraud	32	21	46

The prevalence of payments fraud in 2005 remained about the same as in 2004. Fifty-five percent of organizations reported that the number of attempts at payments fraud was unchanged from the previous year. Large organizations were more likely to experience an increase in payments fraud than smaller organizations. Twenty-nine percent of organizations with annual revenues over \$1 billion report more payments fraud than in 2004. However, just 11 percent of smaller organizations experienced an increase in fraudulent payments activity in 2005 vs. 2004, while almost one-third (30 percent) saw a decrease.

Change in Prevalence of Payments Fraud in 2005 Compared to 2004

(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Increased incidents of fraud	22%	29%	11%
About the same	55	52	59
Decreased incidents of fraud	23	19	30

Checks are the most often used vehicle for payments fraud. Among organizations subject to payments fraud in 2005, 94 percent indicate that they were victims of check fraud.

ACH debits were the second most frequently used method for payments fraud in 2005, with 34 percent of organizations—including nearly 39 percent of large organizations—hit by fraudulent ACH debits. Payment cards accounted for fewer incidents of fraud—13 percent in the case of consumer cards, 10 percent for corporate purchasing cards.

However, organizations have become more effective at fighting back against the criminals. The majority of organizations report that they did not suffer a financial loss as the result of check and ACH debit fraud in 2005. And 85 percent believe that their organization’s reputation was not negatively impacted by attempted or actual payments fraud.

Payment Methods Subject to Fraud in 2005

(Percentage of Organizations that Reported Payments Fraud Activity in 2005)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Checks	94%	97%	91%
ACH debits	34	39	28
Consumer credit or debit cards	13	13	15
Corporate purchasing cards	10	9	13
ACH credits	1	3	*
Wire transfers	1	1	2

Defenses against Check Fraud

Despite the fact that 94 percent of organizations were victims of check fraud, 81 percent of these organizations suffered no financial losses as a result of the attempted fraud. In most cases, the determining factor in whether the organization suffered a loss was positive pay.

Check Fraud Resulting in Financial Loss

(Percentage Distribution of Organizations that Suffered Check Fraud)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Resulted in financial loss	19%	19%	18%
Did not result in financial loss	81	81	82

When asked what fraud control measure was most responsible for preventing financial losses, two-thirds of respondents report that positive pay or reverse positive pay was the primary defense. Another 14 percent attribute loss prevention to payee positive pay. Five percent cite internal factors—daily reconciliation or controls such as separation of duties.

Measure that Prevented Financial Loss from Check Fraud
(Percentage Distribution of Organizations that Suffered Check Fraud Without Loss)

	All Respondents
Positive pay/Reverse positive pay	67%
Payee positive pay	14
Daily reconciliation of balances/transactions	5
Internal controls (e.g., separation of duties)	5
"Post no checks" restriction on depository accounts and/or electronic payment accounts	2
Timely check return	2
Other	6

One in five organizations (19 percent) did suffer a financial loss as a result of check fraud. Twenty one percent of these organizations attribute the loss to their failure to use positive pay or reverse positive pay, while a similar percentage cited lack of payee positive pay. Alteration of payee name appears to have become a more frequent tactic of criminals trying to circumvent positive pay. Internal factors were the second most frequent cause of financial losses. Sixteen percent of organizations report financial losses resulting from employee fraud. Another 16 percent suffered losses because their account reconciliation or check return was not timely.

Primary Reason the Organization Suffered Losses from Check Fraud
(Percentage Distribution of Organizations that Suffered a Financial Loss Resulting from Check Fraud)

	All Respondents
Did not use payee positive pay	21%
Did not use positive pay/reverse positive pay	21
Account reconciliation and/or check return not timely	16
Internal fraud (employee responsible)	16
Did not use other "commercially reasonable" security methods	2
Other	23

Defenses against ACH Debit Fraud

An organization that was a victim of ACH debit fraud was more likely to suffer a financial loss than an organization hit by check fraud. Twenty-seven percent of organizations that report an incident of ACH debit fraud lost money because of the fraud, as opposed to 19 percent of the victims of check fraud.

ACH Fraud Resulting in Financial Loss

(Percentage Distribution of Organizations that Suffered ACH Fraud)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Resulted in financial loss	27%	29%	28%
Did not result in financial loss	73	71	72

ACH debit blocks were the fraud control measure most responsible for preventing losses by targets of ACH debit fraud, cited by 39 percent of organizations. Survey results show that internal controls play a more important role in combating electronic payments fraud than check fraud. The primary defensive measure cited by the second highest percentage of respondents (35 percent) was daily reconciliation or monitoring of balances and transactions. Another 16 percent indicated that they consider ACH debit filters to be primarily responsible for stopping fraud.

Fraud Control Measure Most Responsible for Preventing Loss from ACH Fraud

(Percentage Distribution of Organizations that Suffered ACH Fraud Without Loss)

	All Respondents
ACH debit blocks	39%
Daily reconciliation or monitoring of balances/transactions	35
ACH debit filters	16
Timely ACH return	3
Separate accounts for checks and electronic payments	1
Other	6

When organizations do suffer financial loss from ACH debit fraud, it is primarily because they do not use ACH debit blocks or filters. Forty-four percent of organizations that lost money indicate that it was primarily because they failed to use those tools. Another 20 percent note that their organization did not reconcile their account or return the ACH debit on a timely basis.

Primary Reason the Organization Suffered Losses from ACH Fraud

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

	All Respondents
Did not use ACH debit blocks or filters	44%
Account reconciliation and/or ACH return not timely	20
Internal fraud (employee responsible)	8
Clerical error or inaccurate key entry	4
Other	24

Defenses against Card Payment Fraud

Unlike other types of payments fraud, the majority of organizations that experienced fraud associated with accepting card payments suffered a financial loss. Fifty-four percent of organizations that report an incident of card payment fraud experienced financial losses. Large organizations were more likely to lose money as a result of card payments fraud. Fifty-eight percent of organizations with annual revenues greater than \$1 billion report financial losses compared to 31 percent of organizations with annual revenues less than \$1 billion. In cases of check fraud and ACH debit fraud, there was no difference between large and small organizations in whether losses were incurred.

Card Payments Fraud Resulting in Financial Loss

(Percentage Distribution of Organizations that Suffered Card Payments Fraud)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Resulted in financial loss	54%	58%	31%
Did not result in financial loss	46	42	69

Almost half of respondents (48 percent) report that the fraud control defense most responsible for preventing financial losses associated with accepting card payments is to promptly charge back the fraudulent transaction. Other defensive measures were less often cited as key to combating card payment fraud. Nineteen percent attributed their primary protection to the use of Verified by Visa and MasterCard Secure Card for online transactions. Fourteen percent cited use of an address verification service.

**Fraud Control Measure Most Responsible
for Preventing Loss from Card Payment Fraud**

(Percentage Distribution of Organizations that Suffered ACH Fraud Without Loss)

	All Respondents
Prompt chargeback	48%
Verified by Visa/MasterCard Secure Card	19
Address verification service	14
Use of CVV2 (number on the back of the card)	5
Other	14

If organizations do suffer financial losses from card payments fraud, it is primarily because they are “card-not-present” merchants. Fifty-nine percent of organizations experiencing card payments fraud lost money for this reason. Card-not-present merchants typically conduct their business online or over the phone and assume liability for credit and debit card fraud. Another 28 percent of organizations report suffering losses chiefly because they had not promptly charged back transactions that they had identified as fraudulent.

Primary Reason the Organization Suffered Losses from Card Payments Fraud

(Percentage Distribution of Organizations that Suffered a Financial Loss
Resulting from Card Payments Fraud)

	All Respondents
Card-not-present merchant assumes liability	59%
Delayed chargeback response	28
Other	14

Shifting Payment Methods to Evade Fraud Controls

Because more organizations are using payment-specific fraud controls, criminals might try to evade these defenses by shifting to another payment method. However, only about ten percent of organizations report that attempted or actual fraud resulted from a shift in payment method. In virtually all cases, the shift was from checks to ACH debits. Large organizations are slightly more likely to report fraud attempts as a result of shifting payment methods, perhaps because they have established separate accounts for check and ACH transactions. One organization did report experiencing a financial loss when stolen checks were used to purchase gift cards.

**Fraud Resulting from the Shifting from One Payment Method
to Another to Evade Fraud Controls**

(Percentage Distribution of Organizations that Suffered Payments Fraud)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Yes, organization has experienced such fraud	10%	11%	6%
No, organization has not experienced such fraud	73	71	82
Unknown	17	18	12

Safeguarding Payments Data

An organization’s IT department plays a major role in safeguarding the data of the organization, its vendors and customers. However, many financial professionals have only a moderate understanding of their IT department’s security policies for safeguarding data. Fifty-five percent of respondents “somewhat” understand IT’s security policies, with another 18 percent reporting that they understand security policies “not well at all.” Just over one-quarter of respondents are confident that they understand IT security policies “very well.”

**Understanding of IT Department’s Security Policies
for Safeguarding Organization, Vendor and Customer Data**

(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Very well	27%	28%	28%
Somewhat	55	51	59
Not well at all	18	21	13

Payments Fraud Control Best Practices

Best practice organizations use a wide array of bank-provided payments fraud prevention tools, employ tight internal controls and cooperate across departments to reduce payments risk. Here are some examples:

- “Our Treasury organization has taken a very aggressive stance, employing every possible tool available to us. We work very closely with our Accounting and Reporting group to ensure that fraudulent items are detected early.”

- “We use positive pay, daily reconciliation, payee name verification, secure ink and check stock, ACH debit blocks/filters, three-way matching A/P controls, Master Data controls over vendor setup, full segregation of duties among Master Data, A/P, General Accounting, Treasury and Account Reconciliation.”
- “From a treasury viewpoint, we use all methods available to prevent our accounts from being compromised. We use positive pay, ACH block, segregate payment and receipt accounts, reconcile daily, etc. Operationally, we have a solid IT infrastructure that is well protected and we test our internal controls monthly.”

Internal Controls

Written Payments Policies

The risks to organizations making payments continue to increase in complexity, driven by changes in technology, the variety of payment options available and the number of participants involved in a given payment transaction. Most organizations understand the importance of developing a formal, written payments policy to identify and control these risks, and nearly nine out of ten organizations (88 percent) have such policies.

Organizations with annual revenues greater than \$1 billion are more likely than smaller organizations to have a written payments policy and to update the policy on an annual basis. As an example, one organization reports that “payment controls are revisited periodically and all types of payments and all of the people who have a role in the process are made aware of the potential risk of errors or fraud.”

Organizations that Have a Written Payments Policy

(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Have a written payments policy	88%	92%	83%
Does not have a written payments policy	12	8	17

However in many cases, once an organization has defined its payments policies, they are not frequently revisited. Only thirty-eight percent of organizations update their policies on an annual basis.

Frequency of Updating Written Payments Policies
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Annually	38%	40%	33%
Every other year	8	9	10
Infrequently	35	32	37
Unknown	18	17	13

A comprehensive payments policy is designed to address the full array of risks—fraud, operating and settlement-related—associated with payment initiation, execution and settlement. Procedures are then developed to comply with the payments policy.

When organizations that do not have a written payments policy were asked the reasons why, nearly half indicate that they have a daily procedures manual for payments rather than a policy. Another one-third of respondents report that other management priorities take precedence over the development of a formal policy.

Separation of Duties

The written payments policies of most organizations identify the departments that are authorized to request the payment, authorize the payment and execute the payment. Although requesting departments are less often identified—most likely because of organizational decentralization or diversity—they are specified in 83 percent of policies.

Components of Written Payments Policies
(Percent of Organizations with Written Payments Policies)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Specifies department that can request payments	83%	87%	77%
Specifies department that can authorize payments	97	99	94
Specifies department that can execute payments	95	97	93

In 80 percent of organizations with payments policies, the department that authorizes an electronic payment does not execute the payment. However, in one out of five organizations, the same department can both authorize and execute electronic payments, with the practice slightly more prevalent at smaller organizations.

Department Both Authorizes and Executes Electronic Payments
(Percentage Distribution of Organizations with Written Payments Policies)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization allows practice	20%	18%	23%
Organization does not allow practice	80	82	77

Internal Controls Best Practices

Best practice organizations strictly segregate payments responsibilities. As one organization explained, “our treasury department works closely with internal audit to ensure that segregation of duties is not just an ideal, but a reality.”

Following are examples of procedures reported by survey respondents:

- “Payments requests must be approved by levels of authority in the organization. Persons inputting requests do not approve, authorization is contained to specific users, and executing payments is completed by treasury.”
- “Departments request, comptroller authorizes and treasurer executes.”
- “Payment requests can come from many sources. We have an authorization list for each department specifying who can authorize what payments and up to what amount. Payments are executed by A/P, and the check register is reviewed by corporate accounting. Payments needing wire transfers are given to treasury. There is a wire clearing account monitored monthly by corporate accounting that ensures all wires have been processed through A/P.”

Impact of Sarbanes-Oxley

Despite the significant impact of the Sarbanes-Oxley Act on corporate internal control practices, 46 percent of respondents report that their organization made no material change to its payments controls as a result of Sarbanes-Oxley. Organizations with annual revenues under \$1 billion were much less likely to make changes; 61 percent of smaller organizations report no change compared to 39 percent of larger organizations.

Fifty-four percent of organizations did make material changes to their payments controls as a result of Sarbanes-Oxley. To strengthen their defenses, they now perform more frequent audits (28 percent), require additional approvals (26 percent), or require additional documentation related to the payment request (20 percent).

Impact of Sarbanes-Oxley on Payments Controls
(Percent of Respondents)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
No material change to organization's payments controls	46%	39%	61%
Now performs more frequent audits of payments practices	28	35	26
Now requires additional approvals to request, authorize and/or execute payments	26	27	23
Now requires additional documentation related to the payment request	20	24	22
Other changes	6	5	6

Audit Control Best Practices

To ensure compliance with payments control practices, 53 percent of organizations report that internal and/or external auditors perform surprise audits.

Surprise Audits of Payment Practices
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Auditors perform surprise audits	53%	61%	40%
Auditors do not perform surprise audits	47	39	60

Respondents report:

- “There are both scheduled audits and surprise audits to see that the protocols set forth in the 404 compliance review are active and adhered to.”
- “We had very tight controls on payments prior to SOX, so it was not necessary to add more. Our internal and external auditors have reviewed and approved our controls multiple times. Our internal auditors actually wanted to see live demonstrations of what our written policy states. The only thing they have done is document it on their forms so they can do spot checks more consistently.”

Disaster Recovery

Organizations

The 2005 hurricanes highlighted the vulnerability to natural disasters of payments and other treasury and finance functions. Power or phone outages and hardware or software failures can also prevent organizations from continuing their standard procedures for processing payments and remittances and maintaining liquidity. Fortunately, three-quarters of responding organizations were not affected by natural or systems failures last year. However, about one-quarter of organizations did experience a natural disaster or a power or phone outage in 2005, and 18 percent were impacted by a hardware or software failure.

Organizations that Experienced a Systems Failure in 2005 Due to a Power or Phone Outage or Natural Disaster (Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Had experienced a systems failure	24%	25%	24%
Had not experienced a systems failure	76	75	76

Organizations That Experienced a Systems Failure in 2005 Due to a Hardware or Software Failure (Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Had experienced a systems failure	18%	17%	20%
Had not experienced a systems failure	82	83	80

Twenty-five percent of organizations do not have written disaster recovery plans to manage the operating risks to payments that may result from unanticipated disasters and disruptions. Among those that do have written disaster recovery plans, large organizations are much more likely than smaller organizations. Eighty-one percent of organizations with annual revenues greater than \$1 billion have such plans, compared to 67 percent of smaller organizations.

Organizations with Written Disaster Recovery Plans
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Has a written disaster recovery plan	75%	81%	67%
Does not have a written disaster recovery plan	25	19	33

The majority of organizations with disaster recovery plans test them on a frequent basis. Fifty-seven percent test their plans at least annually. On the other hand, more than a third of organizations (35 percent) only test their plans infrequently.

Testing Frequency of Written Disaster Recovery Plans
(Percentage Distribution of Organizations with Disaster Recovery Plans)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Every six months	13%	14%	14%
Every year	44	48	41
Every two years	8	6	9
Infrequently/never	35	33	35

Most organizations use their own off-site facility to initiate and execute payments in the event of a disaster or systems failure at their customary location. Twenty percent use a bank's facility for back-up, while nine percent use a third-party location. Others either do not have back-up facilities or operate from employees' homes.

Provider of Back-Up Processing Facility for Initiating and Executing Payments in the Event of Systems Failure at Your Organization
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization's own off-site/redundant facility	61%	62%	59%
Bank's facility	20	19	21
Third party facility	9	11	7
Other	10	9	12

The ability to resume payments activities quickly after a systems failure is critical. Sixty-five percent of organizations indicate that their back-up facility can be operational in a half day or less. Sixteen percent of organizations need a full day to activate their back-up facility, while seven percent need at least two days to be able to initiate and execute payments from a back-up site.

Time Needed for Back-Up Facility to Become Operational
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
1-2 hours	38%	39%	37%
Half-day	27	28	26
One day	16	16	15
Two or more days	7	8	6
Other	11	10	15

Alternative procedures that are used when primary systems fail or in the event of a disaster are often manual, have different risks and may require special internal controls. Disaster recovery plans should ensure that controls are in place to manage the specific risks associated with back-up processes.

Fifty-eight percent of organizations have designated back-up personnel to initiate and execute payments in the event regular staff is not available. However, less than half of organizations (44 percent) have authorization and approval procedures specifically for employees working off-site or at home, and they are more likely to be larger organizations.

**Designated Back-up Personnel to Initiate and Execute Payments
in the Event that Regular Staff is Not Available**
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization has designated back-up personnel	58%	60%	55%
Organization has not designated back-up personnel	42	40	45

**Authorization and Approval Procedures Specifically
for Employees Working Off-Site or at Home**
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Organization has procedures specifically for employees working off-site or at home	44%	49%	39%
Organization does not have procedures specifically for employees working off-site or at home	56	51	61

Banks and Third-Party Processors

Systems failures at banks and third-party processors may also interfere with an organization's payments processes. In 2005, 13 percent of organizations reported that they lost productive time or were unable to meet their financial obligations because of a systems failure at their bank or third-party processor.

**Organization's Payments Processes Disrupted in 2005 Because of a Systems
Failure at a Bank or Third-Party Processor**
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Had experienced disruption	13%	14%	12%
Had not experienced disruption	73	74	71
Unknown	14	12	17

Because of the critical role that banks and third-party providers play in the payments process, organizations should inquire about their processors' contingency plans and back-up facilities. However, less than half of organizations—45 percent—indicate that their banks have communicated to them their disaster recovery plans for processing payments in the event of a disaster at the bank. Large organizations are more likely to receive this information, with 51 percent of organizations having annual revenues greater than \$1 billion receiving such information compared to just 35 percent of smaller organizations.

Communication by Banks About Their Disaster Recovery Plans
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Banks have communicated plans	45%	51%	35%
Banks have not communicated plans	55	49	65

Most organizations that receive this information are relatively satisfied with the response. Three out of five organizations (59 percent) are either satisfied or very satisfied with their banks' disaster recovery plans, while another 35 percent are "somewhat satisfied"

Satisfaction with Banks' Disaster Recovery Plans
(Percentage Distribution)

	All Respondents	Revenues over \$1 billion	Revenues under \$1 billion
Very satisfied	13%	11%	16%
Satisfied	46	48	42
Somewhat satisfied	35	36	31
Dissatisfied	6	5	8
Very dissatisfied	1	*	4

Disaster Recovery Best Practices

Best practice organizations understand that contingency plans to control payments risk and resume payments operations in the event of a disaster or systems failure must have two key components: specific internal controls and frequent testing.

Here are examples of how best practice organizations manage their disaster recovery planning:

- “Each electronic payment initiator must test their home PC's digital certificate quarterly and submit a form with proof of that test. Telephone initiation wire instructions, tracking mechanisms and contact phone numbers are written within the policy. All back-up and tracking spreadsheets must be forwarded to the treasury manager weekly for verification purposes.”
- “We have a strong commitment to DR/BCP that began as we prepared for Y2K. We test at least once a year, update at least quarterly, and are continually evolving our plan to reflect the evolution of the organization.”
- “Our plan is tested regularly, in different ways, by IT, by the bank, by internal auditors, and by independent third party consultants. Each brings a different point of view to the testing. Recommendations are weighed and discussed before being accepted, rejected, or modified.”
- “We have tiers of operations that must be up and running by certain times following a disaster/service outage. Payments are in the top tier (1-2 hours). We have fully automated our electronic payments process so that it can be handled from anywhere with Internet access. For check processing we have one redundant site. If both sites are not available we will substitute electronic payments or credit card payments to resolve urgent issues.”

Conclusions

Organizations in 2005 faced significant risks to the security and continuity of their payment systems from fraud, from natural disasters and from systems failures. Payments fraud last year was widespread and broad-based, and the Gulf Coast hurricanes highlighted the vulnerability to natural disaster of all finance functions. However, the AFP survey reveals that the majority of organizations have built strong defenses to mitigate fraud and operating risk. Best practice organizations use a wide array of bank-provided payments fraud prevention tools, employ tight internal controls and cooperate across departments to reduce payments risk.

Despite the prevalence of fraud, the majority of organizations did not suffer financial loss in 2005 as the result of check and ACH debit fraud. The primary defenses against check fraud are positive pay and reverse positive pay. Victims of ACH debit fraud find debit blocks to be most responsible for preventing loss. In the case of card payments, prompt chargeback is the most used defense against loss, but “card not present” merchants continue to suffer losses because of liability rules for those who conduct business online or over the phone.

To strengthen internal controls against both fraud and operating risk, nearly nine out of ten organizations have developed written payments policies. Included in the policies of these best practice organizations are requirements for strict segregation of payments responsibilities among departments.

Three quarters of organizations have written disaster recovery plans. The majority test their plans frequently and have designated back-up personnel to initiate and execute payments in the event regular staff is not available.

However, many organizations continue to be exposed to risk because of their delay in adopting best practices. In some cases, these organizations are smaller organizations with annual revenues less than \$1 billion, but they can nevertheless be vulnerable to the same types of risks that face larger organizations.

A number of organizations have not yet implemented positive pay to control check fraud. Use of payee positive pay will become more critical as criminals increasingly attempt to alter payee names. Organizations should become more aware of the role of ACH debit blocks and filters in preventing electronic payments fraud.

Survey responses also highlight the need for finance, treasury and IT departments to work together to strengthen their organizations’ security policies for safeguarding financial as well as customer and vendor data. With the passage of data security and breach notification laws by state and federal governments, organizations will face increased liability for leaks of sensitive information.

To strengthen internal controls, organizations that have developed written payments policies should review and update them frequently. New payments options, the merging of payment methods and changing patterns of consumer and corporate payment usage call for increased senior management focus on payments risk management. Treasury should also involve the organization’s audit staff to ensure that internal controls do not lag changes in payments practices.

Finally, many organizations (25 percent) lack written disaster recovery plans. Among those that have such plans, more than a third of organizations only test their plans infrequently. Should a natural disaster or system outage affect their organization, less than half of organizations (44 percent) lack internal controls—for example, payments authorization and approval procedures—specifically for employees working off-site or at home.

By highlighting best practices, AFP hopes to promote awareness by treasury and finance professionals and encourage their more widespread use.

About the survey

In February 2006, the Association for Financial Professionals sent a survey to 3,000 corporate practitioner members about payments risks impacting their organization. The survey contained questions on payments fraud, internal controls in payments activities and disaster recovery plans for their payments operations. The survey was sent to AFP corporate practitioner members with these job titles: cash managers, analysts, assistant treasurers, directors and controllers. After eliminating surveys sent to invalid and/or blocked email addresses, the 352 responses yield an adjusted response rate of 12 percent. AFP also sent the survey to prospective members holding similar job titles and generated an additional 48 responses. Detail presented in tables may not add to 100 due to rounding.

Financial professionals who responded to the survey on behalf of their organizations are representative of AFP's membership as a whole. The typical respondent works for an organization with annual revenues slightly higher than \$1 billion. The largest percentage of respondents is employed in manufacturing, followed by retail, energy, and insurance.



About the Association for Financial Professionals

The Association for Financial Professionals (AFP) headquartered in Bethesda, Maryland, supports more than 14,000 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