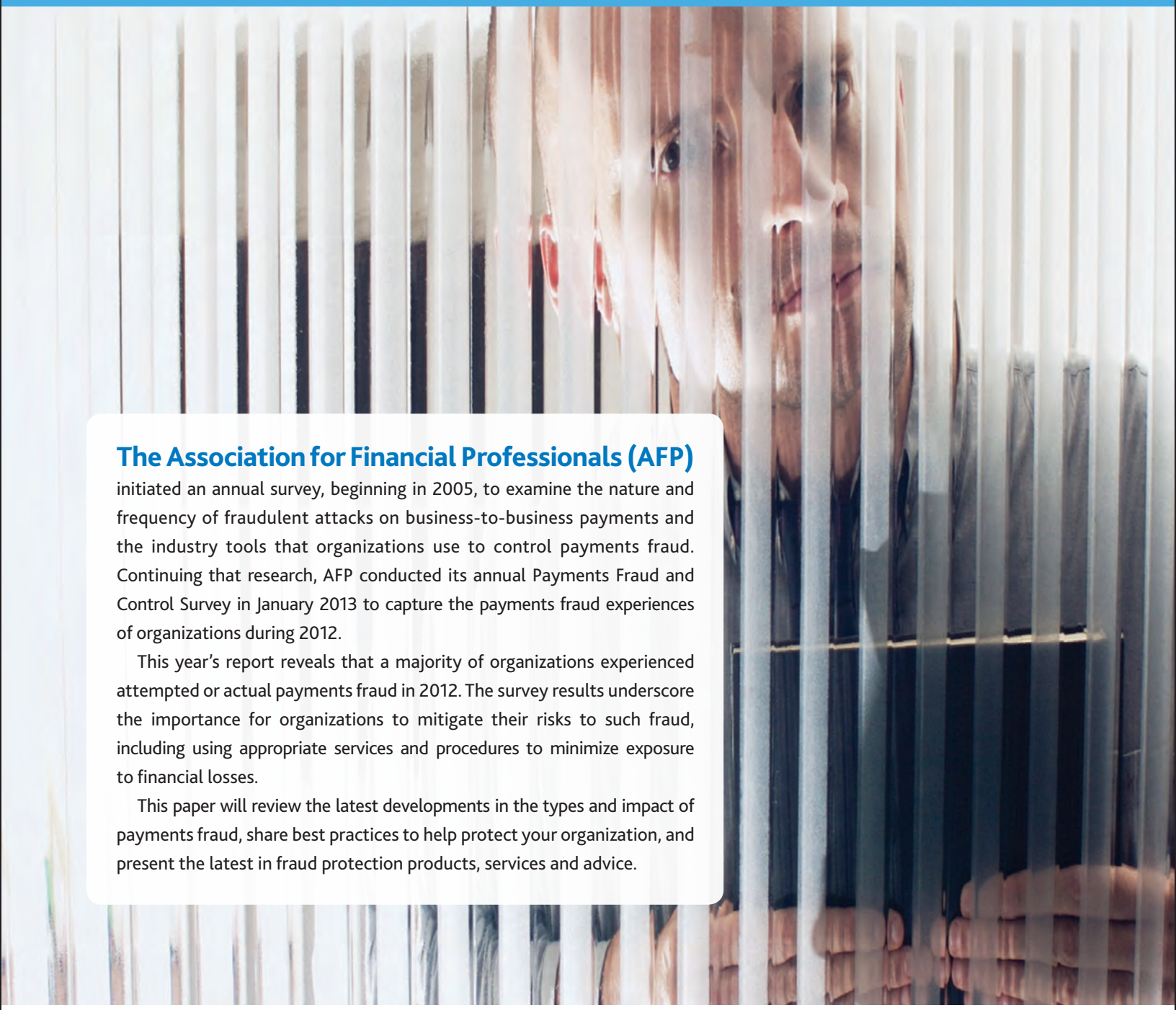
CHASE Paymentech™

WHITEPAPER

Payments Fraud: Down but Not Out

Findings based on the 2013 Payments Fraud and Control Survey conducted by the Association for Financial Professionals (AFP) and sponsored by JPMorgan and Chase Paymentech.



The Association for Financial Professionals (AFP)

initiated an annual survey, beginning in 2005, to examine 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, AFP conducted its annual Payments Fraud and Control Survey in January 2013 to capture the payments fraud experiences of organizations during 2012.

This year's report reveals that a majority of organizations experienced attempted or actual payments fraud in 2012. The survey results underscore the importance for organizations to mitigate their risks to such fraud, including using appropriate services and procedures to minimize exposure to financial losses.

This paper will review the latest developments in the types and impact of payments fraud, share best practices to help protect your organization, and present the latest in fraud protection products, services and advice.

Table Of Contents

The Fraud Factor

In 2012, 61 percent of organizations experienced attempted or actual payments fraud – down from 66 percent in 2011 and 71 percent in 2010. However, fraud is still higher than the 55 percent level reported in the initial Association for Financial Professionals (AFP) survey on the topic (conducted in 2005, reflecting activity in 2004).[1]

Even with recent declines, it is important to keep in mind that any amount of fraud is still too much. The facts from AFP reveal that threats are ever-present:

- Twenty-six percent of survey respondents report that incidents of fraud increased in 2012 from 2011, while 16 percent experienced a decrease and 58 percent saw no change.
- Twenty-seven percent of organizations that were victims of actual and/or attempted payments fraud in 2012 experienced actual financial loss – up from 26 percent in 2011.
- All payment types continue to be impacted, and in 2012 commercial/corporate purchasing card fraud surpassed that for ACH debits.

Figure 1.0

PERCENT OF ORGANIZATIONS SUBJECT TO ATTEMPTED OR ACTUAL PAYMENTS FRAUD IN 2012

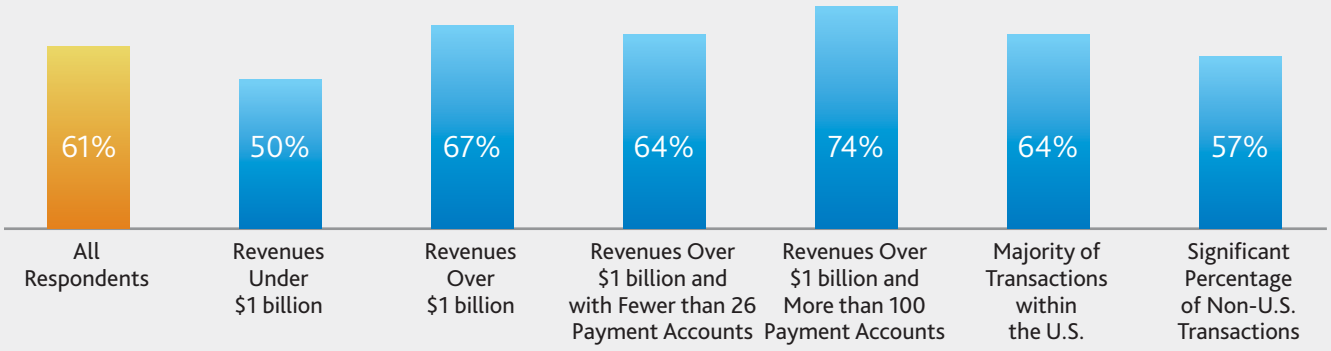
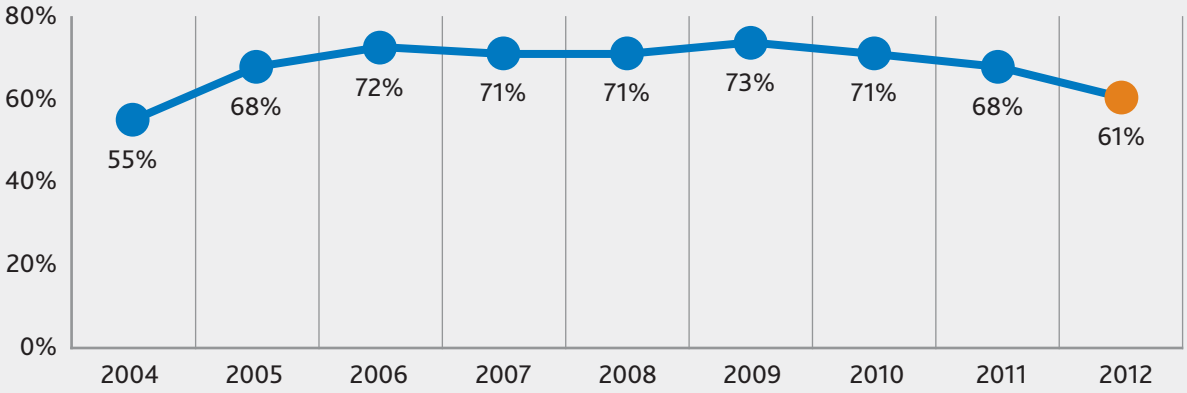
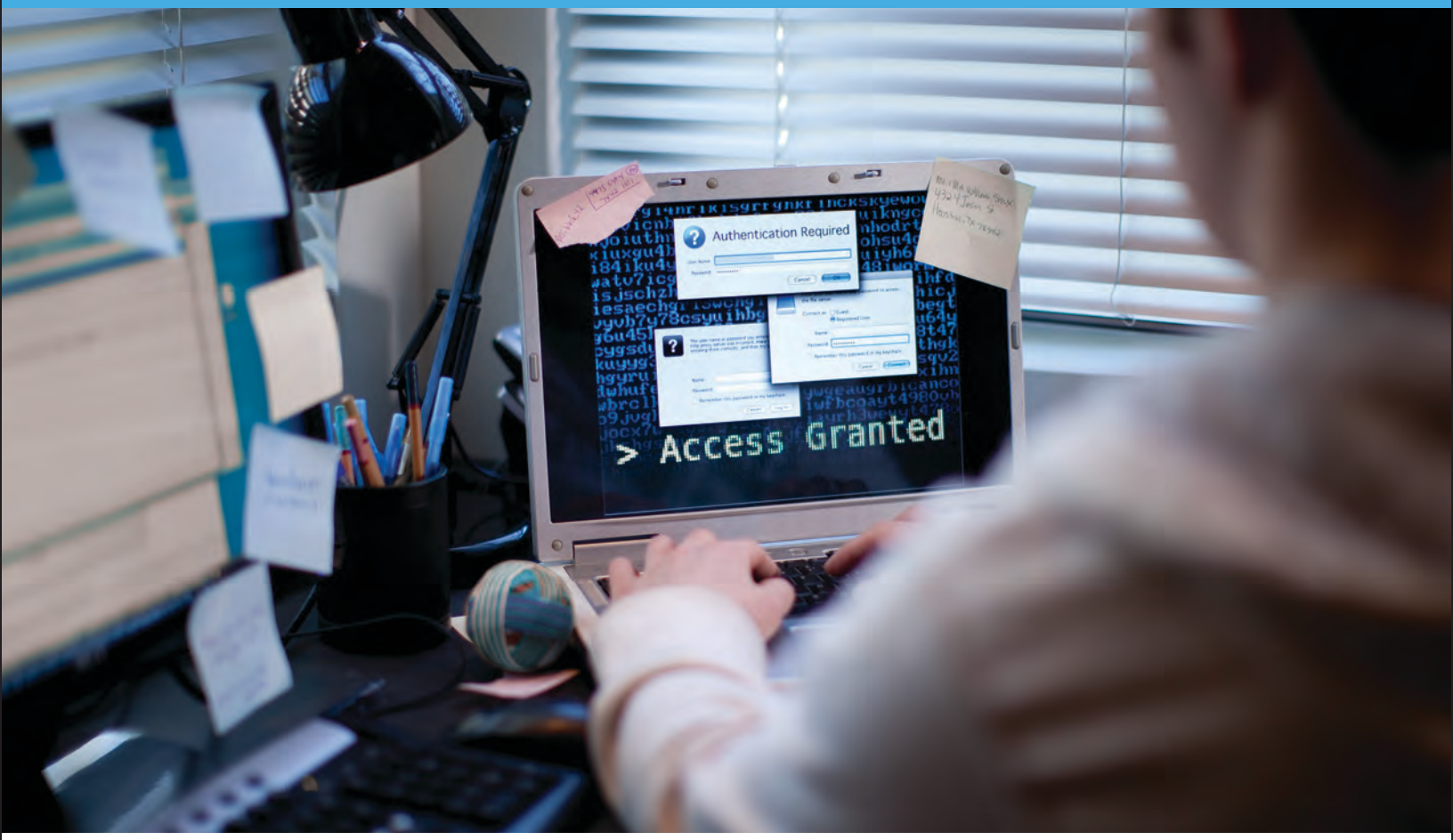


Figure 2.0

PERCENT OF ORGANIZATIONS SUBJECT TO ATTEMPTED AND/OR ACTUAL PAYMENTS FRAUD





The Fraud Factor *continued*

Company size and domicile of payments are often defining factors. Specifically, 67 percent of organizations with annual revenues over $1 billion were victims of payments fraud, compared to half of those with annual revenues under $1 billion.

Organizations with a large number of payment accounts were even more likely to be exposed to payments fraud in 2012. Seventy-four percent of organizations with annual revenues over $1 billion and more than 100 payment accounts were subject to payments fraud in 2012, compared to the 64 percent of similarly-sized organizations with 25 or fewer payment accounts.

The survey also revealed that companies which perform a significant number of non-U.S. transactions generally experience more fraud.

Fortunately, evolution has continued in fraud prevention techniques, technology, products and services. Plus, no matter how sophisticated a particular tool may be, there is no substitute for personal dialogue and guidance – an area surveyed presents an opportunity to leverage the expertise of banking partners:

- Less than half, 45 percent, of respondents reported discussing payment fraud at least once with a bank counterpart in treasury services in 2012.
- Only 14 percent discussed fraud with a bank's product manager or a technical/security contact at least once in 2012.
- Five percent more had discussions with their banks and agreed to or changed security procedures in 2012.

Even with recent declines, it is important to keep in mind that any number greater than zero – for any measure of fraud – is too much.

Payment Forms

Predictably, checks continue to lead the pack in terms of the percentage of organizations affected by attempted and actual fraud, as well as the severity of actual losses. Check fraud increased slightly, from 85 percent in 2011 to 87 percent in 2012.[2] The remainder of payment forms experienced considerably less fraud. An interesting development is the switch in places of ACH debits and corporate/commercial purchasing cards. Clients should note the dramatic year-over-year fraud increases for each of these payment types.

- **Corporate/commercial purchasing cards:** 29 percent in 2012, up from 20 percent in 2011
- **ACH debits:** 27 percent in 2012, up from 23 percent in 2011
- **Wire transfers:** 11 percent in 2012, up from five percent in 2011
- **ACH credits:** Eight percent in 2012, up from five percent in 2011

PERCENT OF ORGANIZATIONS SUBJECT TO ATTEMPTED OR ACTUAL PAYMENTS FRAUD IN 2012

	All Respondents	Revenues Under $1 billion	Revenues Over $1 billion	Revenues Over $1 billion and with Fewer than 26 Payment Accounts	Revenues Over $1 billion and More than 100 Payment Accounts	Majority of Transactions within the U.S.	Significant Percentage of Non-U.S. Transactions
CHECKS	87%	87%	91%	93%	94%	92%	87%
CORPORATE/COMMERCIAL CARDS	29	27	26	23	34	18	32
ACH DEBITS	27	25	29	27	36	31	24
WIRE TRANSFERS	11	7	12	5	19	8	10
ACH CREDITS	8	9	6	2	15	5	7

Figure 3.0

Payment Forms *continued*

Checks

According to the Federal Reserve's 2010 Payments Study, an every-three-year report, checks account for nearly 20 percent of all non-cash payments.[3]

Although the Fed reports a decrease in the average value of checks paid,[4] those continue to represent larger dollar transactions, particularly in business-to-business (B2B) payments. Increasingly sophisticated and affordable printing technology continues to make altering and counterfeiting checks a relatively low-cost enterprise for fraudsters.

Corporate/Commercial Purchasing Cards

Organizations continue to adopt corporate/commercial cards for (B2B) payments. The three most widely used B2B cards in 2012 were:[5]

- **Purchasing cards:** used by 84 percent versus 75 percent in 2011
- **Travel and entertainment (T&E) cards:** 58 percent versus 38 percent in 2011
- **Ghost or virtual cards:** 48 percent versus 23 percent in 2011

These too are targets for fraud – whether via external or internal misuse, embezzlement and/or dishonesty – though fortunately the instances are on the decline:

- Almost half of the organizations surveyed by AFP experienced fraud during 2012 through the use of their own corporate/commercial cards – a decrease from 55 percent in 2011.
- Nearly three quarters of respondents (74 percent in 2012 versus 81 percent in 2011) reported that the fraud was committed by an outside party.
- The proportion of organizations reporting incidents of employee-perpetrated fraud decreased from 38 percent in 2011 to just 26 percent in 2012. Fortunately, that figure is even lower than the 29 percent reported in 2010.[6]

ACH

While the percentage of companies experiencing ACH fraud is on the rise, when it does happen, it usually is infrequent at individual organizations. Sixty-four percent of those subject to ACH fraud report between just one and five instances in 2012.

Since clients, not banks, most often are the initial target of ACH fraud, mitigating fraud primarily falls to the company. Learning from treasury peers, the most likely reasons why an organization sustained financial losses from ACH fraud include:

- Untimely account reconciliation
- No use of ACH debit blocks or filters
- Untimely return of ACH item
- Did not use ACH Positive Pay

As ACH transactions proliferate, so do the accompanying fraud schemes:

- **Account Hijacking:** Fraudsters use stolen client credentials to login, quickly withdrawing money before the fraud is uncovered.
- **Identity Fraud:** Criminals create false identities, deceive their way into obtaining ACH origination capabilities and then initiate fraudulent debits.
- **ACH Kiting:** An ACH debit is originated from one account and drawn on another, with the available balance taken out before settlement.
- **Reverse Phishing:** Perpetrators send corporations e-mails containing alternate banking information that redirects ACH payments to a fraudulent account.
- **Insider Origination Fraud:** Employees at a merchant or bank manipulate an ACH origination file to skim funds from a company.
- **Counterfeiting:** ACH debits are generated through electronic conversion of a counterfeit check.

Financial Losses and Perpetrators of Fraud

Payments fraud attempts resulted in varying amounts of both potential and actual losses – and originated from an array of sources.

Potential Loss – Of the organizations that experienced payments fraud in 2012, only eight percent estimated the potential loss as zero. For 37 percent, the projected loss was less than $25,000 and 38 percent projected that to be between $25,000 and $249,999.

Actual Loss – Fortunately, nearly three-quarters of organizations that experienced at least one payments fraud attempt in 2012 did not suffer any actual losses. This is largely due to effective fraud detection and controls. Another 16 percent realized a financial loss of less than $25,000, while 11 percent reported a loss in excess of $25,000. The median actual loss was $20,300.

Payment Methods – While the occurrence of actual financial loss – regardless of the sum – is more likely with cards, checks by far result in the largest realized dollar amounts of losses.

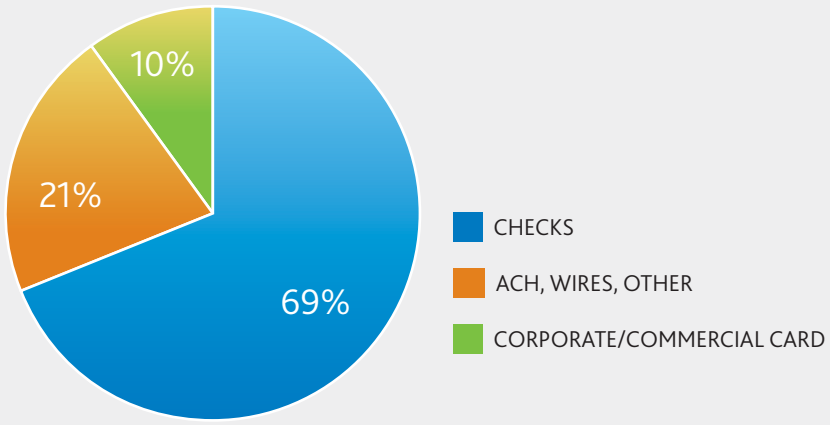
The percentage of organizations suffering any amount of actual financial loss from corporate/commercial card fraud is 26 percent, while checks represent 16 percent and ACH 12 percent.

Cost to Manage, Defend and/or Clean-Up – For most organizations that were subject to attempted or actual payments fraud in 2012, the cost to manage, defend and/or "clean-up" from the events was relatively modest.

Perpetrators of Fraud – The vast majority of organizations that experienced attempted and/or actual payments fraud in 2012 were affected as a result of actions outside the company.

Figure 4.0

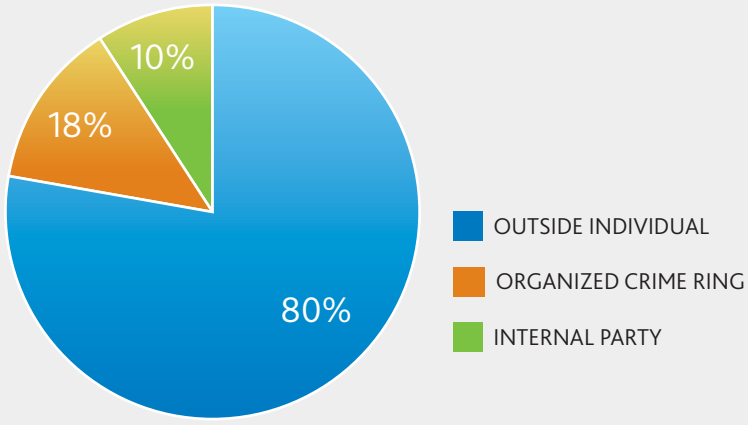
PAYMENT TYPE RESPONSIBLE FOR GREATEST ACTUAL FINANCIAL LOSS



The percentage of organizations suffering any amount of actual financial loss from corporate/commercial card fraud is 26 percent, while checks represent 16 percent and ACH 12 percent.

Figure 5.0

THE THREE HIGHEST PERPETRATORS OF FRAUD



Forty percent of the organizations did not face any expenses in relation to the fraud. Slightly less than half (45 percent) of affected organizations spent less than $25,000. Only three percent paid more than $50,000.

Best Practices

Overall effective treasury practices include daily reconciliation, prompt return of unauthorized items and segregation of accounts. For the latter, 74 percent of organizations in 2012 did that both for payment types (e.g., wire, ACH, check) and by purpose (e.g., taxes, payroll). Allowing for more timely and focused review of payment activity, the most popular separations included:

- **Disbursement and collections:** 65 percent
- **By payment purpose:** 58 percent
- **Wire transfers:** 33 percent
- **Receiving ACH debit payments:** 24 percent

Related opportunities include segregating paper from electronic transactions and high-volume accounts from low-volume ones.

Checks

- Use high-quality check stock with built-in security features, including fluorescent fibers, watermarks, chemical resistance, bleach-reactive stains, thermo-chromatic ink, endorsement backer, micro printing, warning band border, etc.
- Purchase check stock from known vendors.
- Establish an employee order/re-order policy for check stock.
- Securely store check stock, deposit slips, bank statements and canceled checks.
- Implement dual controls over check stock, check issuance and account reconciliation.
- Ensure secure financial document destruction processes.

Corporate/Commercial Purchasing Cards

- Secure senior management to champion your card compliance program and foster company buy-in.
- Create checks and balances via logical segregation of responsibilities, e.g., purchase requests, authorization and execution.
- Support consistency across the organization for card issuance, transaction controls, usage, documentation and record retention.
- Mandate training for all card users and managers.
- Establish protective controls, such as transaction and monthly limits, as well as the blocking of unauthorized vendors.
- Partner with an issuer that provides enhanced reporting and real-time spending visibility.
- Audit for red flags beyond just spending limits, such as off-hour and personal-type purchases.
- Foster cooperation and an interactive environment that encourages employee/cardholder feedback.
- Conduct peer reviews before official audits to mitigate improper card usage and help support regulatory requirements.
- Network to validate business direction and philosophy, plus learn valuable lessons from peer program administrators.

ACH

- Know who you are dealing with – fraud thrives in instances in which an organization believes the perpetrator is legitimate.
- Mask account numbers and tax ID numbers in your correspondence.
- Use encrypted email for confidential, non-public information.
- When an employee leaves the company, ensure that SecurID® tokens are collected and passwords are changed.

Overall effective treasury practices include daily reconciliation, prompt return of unauthorized items and segregation of accounts.

Best Practices *continued*

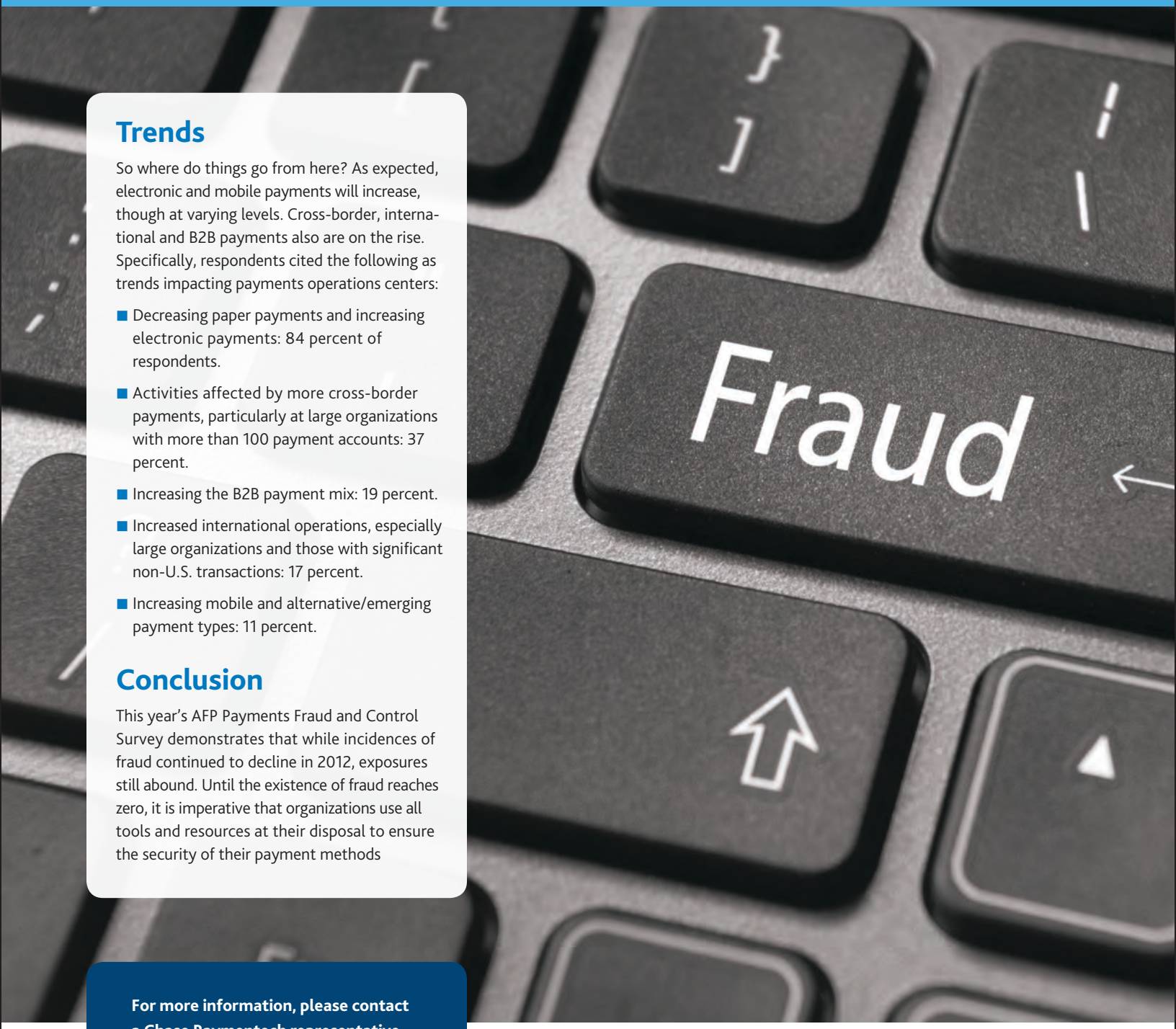
Electronic Protection

Though basic, the precautions below are extremely effective when in effect:

- Ensure your browser and security software are updated, including anti-virus software, firewall protection and software patches.
- Always type a bank's address into your browser rather than clicking links in emails.
- Make certain that staff logs out of online sessions when they step away from their computers.
- Install spam-blocking filters and maintain company-wide surfing block controls.
- Consider blocking plug-ins and pop-ups on computers used for online banking.
- Maintain separate e-mail addresses for personal and business use.
- Confirm your firm's policies, practices and incident processes regarding potential fraudulent activity, update them regularly and ensure all necessary staff are aware.
- Know how to use your firm's resources for forensic and incident response, investigation and disaster recovery so you can respond quickly and effectively to any threat of fraud.
- Train, educate, test and reward your staff for adhering to all of the above.

Bank Security

The better your bank is at providing the latest in fraud protection, the less risk there is to your organization. Among the topics you should discuss with your banking partner(s) are fraud monitoring and detection systems, encryption techniques, multi-factor authentication models, dual-authority models and/or step-up authentication for transactions, and client education training, programs and support.



Trends

So where do things go from here? As expected, electronic and mobile payments will increase, though at varying levels. Cross-border, international and B2B payments also are on the rise. Specifically, respondents cited the following as trends impacting payments operations centers:

- Decreasing paper payments and increasing electronic payments: 84 percent of respondents.
- Activities affected by more cross-border payments, particularly at large organizations with more than 100 payment accounts: 37 percent.
- Increasing the B2B payment mix: 19 percent.
- Increased international operations, especially large organizations and those with significant non-U.S. transactions: 17 percent.
- Increasing mobile and alternative/emerging payment types: 11 percent.

Conclusion

This year's AFP Payments Fraud and Control Survey demonstrates that while incidences of fraud continued to decline in 2012, exposures still abound. Until the existence of fraud reaches zero, it is imperative that organizations use all tools and resources at their disposal to ensure the security of their payment methods

For more information, please contact a Chase Paymentech representative.

1. Association for Financial Professionals. 2005 and 2013 AFP Payments Fraud and Control Surveys.
2. 2012 AFP Payments Fraud and Control Survey.
3. Federal Reserve System. December 18, 2010. The 2010 Federal Reserve Payments Study: Noncash Payment Trends in the United States: 2006 - 2009. Updated April 2011.
4. The 2010 Federal Reserve Payments Study.
5. 2011 and 2012 AFP Payments Fraud and Control Surveys.
6. 2010, 2011 and 2012 AFP Payments Fraud and Control Surveys.