RISK MITIGATION

Safeguarding your organization

April 2012

J.P.Morgan

Today's agenda

- Today I will be covering:
- Latest Payment Fraud Statistics
- Best Practices for Fighting Fraud:
  - What You Can Do Internally
  - How Chase Can Help
- Leading Fraud Prevention Tools
- Client Case Study

Mitigating the risk of payments fraud

Chase takes fraud very seriously—the protection of our client's accounts and financial information is one of our top priorities

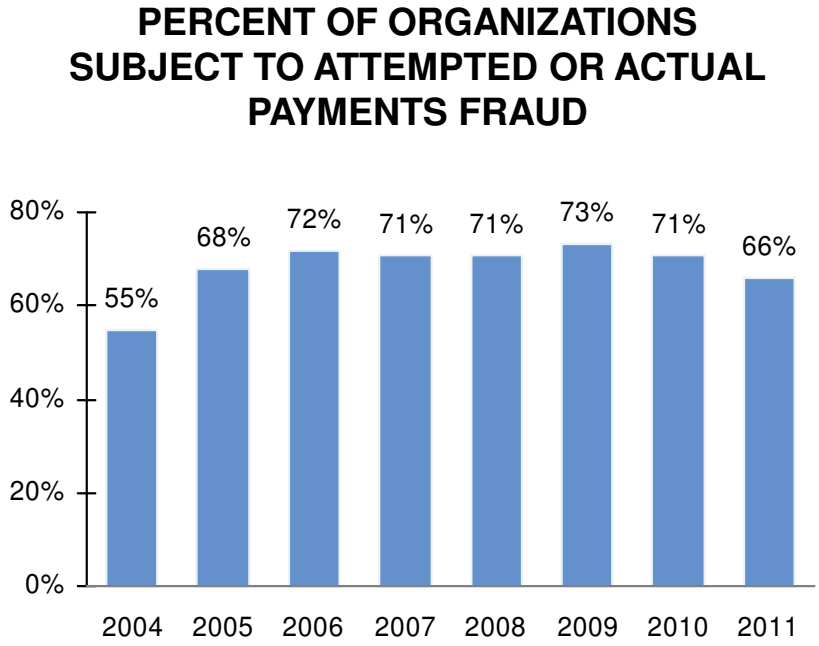
- The best way to protect your business against fraud is to have a plan in place before the problem occurs
- With a combination of strict internal controls and account protection services, you can significantly reduce your exposure to payments fraud

> *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 those financial and treasury professionals responsible for protecting the assets of their organizations.*
>
> **— 2012 AFP PAYMENTS FRAUD AND CONTROL SURVEY**

Source: 2012 AFP Payments Fraud and Control Survey http://www.afponline.org

Payments fraud is a growing problem…

- 66% of organizations experienced attempted or actual payments fraud in 2011 – within the range observed over the past five years.[1]
- 81% of organizations with annual revenues over $1 billion were victims of payments fraud.
- 55% of organizations with annual revenues under $1 billion were victims of payments fraud.
- 28% of organizations report that incidents of fraud increased.
- The median loss of organizations that sustained any financial losses resulting from payments fraud was $19,200.



[1]Source: 2012 AFP Payments Fraud and Control Survey http://www.afponline.org

…and is widespread

- Growth in check fraud has far outpaced the growth in electronic payment fraud
- Of organizations that experienced attempted or actual payments fraud, 85% specified check fraud – high percentage (90%) reported from larger organizations
- Corporate card fraud (15% in 2010 to 20% in 2011) has overtaken consumer credit/debit card fraud (23% to 12%)

Additional reasons for proliferation of check fraud:

- Easy-to-commit, quick-hit crime – increase in organized professional fraud rings
- Requires no special skills
- Technology-assisted crime (scanners, printers, desktop publishing software)

PREVALENCE OF FRAUD BY PAYMENT METHOD

(Percent of organizations)

	All Organizations	Rev. under $1 billion	Rev. over $1 billion
Checks	85%	82%	90%
ACH debits	23%	27%	22%
Corporate purchasing cards	20%	22%	20%
Consumer credit/ debit cards	12%	13%	11%
ACH credits	5%	4%	5%
Wire transfers	5%	4%	4%

Source: 2012 AFP Payments Fraud and Control Survey http://www.afponline.org

Fraud diagnostic tool

Check

Scenario – Product / Encashment	Limit	TS Rating	CB Rating	Proposed Rating	Rationale
Post No Check	n/a	**Low**	**Low**	**Low**	
Positive Pay only	Up to 10k	**Med**	**Low**	**Med**	Low risk implies no action but we recommend adding Payee Name.
Positive Pay only	Over 10k	**High**	**Low**	**Med**	
Positive Pay with Payee Name	Up to 10k	**Low**	**Low**	**Low**	Encashment limit is no longer considered when PP w/PN is in place.
Positive Pay with Payee Name	Over 10k	**Med**	**Low**	**Low**	
Reverse Positive Pay	Up to 3k	**Med**	**Med**	**Med**	Encashment limits serve to limit loss amounts if fraud occurs but PNC or PP w/PN could have prevented the fraud in the first place. RPP is a 2nd day process and therefore more open for fraud than PP w/PN.
Reverse Positive Pay	3k up to 10k	**Med**	**Med**	**High**	
Reverse Positive Pay	Over 10k	**High**	**Med**	**High**	
No products	Up to 10k	**Very High-3**	**Med**	**Very High**	Accounts with no services, regardless of encashment limit, are highest priority to address.
No products	Over 10k	**Very High-4**	**High**	**Very High**	

ACH

Scenario	Rating (no change)
Debit Block or Transaction Review	**Low**
No products	**High**

- "High" is a subjective term – not the same relative risk as a "high" Check rating but means there is an opportunity to close a potential gap

- The account level rating appears on the intranet tool and in client reports to show the relative priority and ease of available actions to take

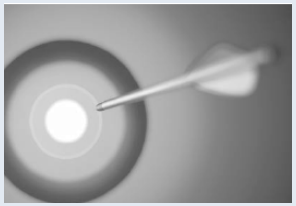
RISK MITIGATION

Best practices for fighting fraud – a comprehensive approach

The right plan includes good controls within your operations and a strong partnership with your bank.

What You Can Do				How We Can Help
Paper	**Electronic**	**Internal Controls**	**Online Security**	**Our Solutions**

▪ Use high security check stock.
▪ Securely store check stock, deposit slips and bank statements.
▪ Implement secure financial documentation destruction processes.
▪ Outsourcing check print – it's more efficient, safer and reduces fraud exposure
	▪ Use an online banking system for treasury.
	▪ Convert paper to electronic, where possible.
	▪ Establish policies on use of executive signatures on electronic documents.
	▪ Collect Secure ID tokens and change passwords when employees leave.
		▪ Segregate duties:
		  ▪ Making payments vs. reconciling accounts
		  ▪ Creating vs. approving vs. releasing wires.
		▪ Monitor & reconcile accounts daily.
		▪ Use online statements, reporting & reconcilement services to speed the reconciliation process.
			▪ Mask Tax IDs correspondence.
			▪ Use encrypted e-mail for confidential, non public information.
			▪ Maintain an awareness of the latest fraud trends, such as phishing and malware.
				▪ Maintain separate accounts for:
				  ▪ Collections & disbursements
				  ▪ Check & electronic payments
				▪ Implement J.P.Morgan fraud mitigation solutions:
				  ▪ Positive Pay with Payee Name Verification
				  ▪ ACH Debit Block
				  ▪ ACH Transaction Review

RISK MITIGATION

J.P.Morgan

Paper checks – *best practices*

In addition to moving to electronic payments, you can mitigate paper check fraud loss by:

- Using high-quality, blank check stock with built-in security features which may include:
  - Fluorescent fibers, watermark, chemical resistance, bleach-reactive brown stain, photocopy void pantograph, endorsement backer, thermo-chromic ink, micro printing, warning band border, laid lines, non-negotiable mark
- Purchasing stock from approved vendors
- Securely storing check stock and controlling access
- Leveraging electronic forms of financial documents such as deposit slips, bank statements and cancelled checks.
- Implementing a secure Financial document destruction process
- Establishing employee order/re-order policy for stock
- Outsourcing check print – it's more efficient, safer and reduces fraud exposure

Check print outsourcing

Key Benefits

- Eliminate the cost of in-house printing, equipment maintenance, paper stock and storage. Take advantage of our pre-sort postage discounts.
- Free your company's resources to focus on core competencies.
- Increase quality of data security, and fraud controls with a single file to provider with automated Positive Pay system updates.
- Leverage industry regulations for MICR and Image quality.
- Leverage web-based check print services that allows the user to setup and test check templates and file formats.
- Accommodates moving from checks to electronic payments via a single mixed payment file.
- Reduce your vulnerability and downtime if a disaster should occur.
  - Print and mail operations is an important aspect of DR Plans

Consider Electronic Payments!

Leading-edge fraud protection

Positive Pay reconciles checks presented for payment against checks issued by you, Items that don't match your issue file information are sent to you as exceptions for decision and are available for review each morning via our Internet-based Web Payables Service.

Payee Verification enhances Positive Pay by identifying potential fraudulent checks when only the payee name has been altered.

- *Maximum Dollar Threshold* enables you to control checks posting to your account based on your established dollar threshold limit.
- *Stale-Dating* enables you to define the number of days after the issue date that a check may be honored. Checks that come in after the defined number of days will be returned automatically as stale-dated items, or can be referred to you for a pay or return decision
- *Check Cashing* with Positive Pay protection prevents fraudulent checks from being cashed on your account at JPMorgan Chase branches.

- Reverse Positive Pay sends you to an online queue of all checks (or a pre-defined subset of checks) that were presented for payment in the last 24 hours. You review for any discrepancies, then instruct us to pay, return or adjust the dollar amount.
- Post No Checks prevents all check debits from posting against your account.

Teller check cashing controls

How it Works

- Teller line protection that prevents all checks, or checks above a specified amount, from being cashed against a Chase account by non-customers

Options

- No Check Cashing: Teller line protection that prevents checks from being cashed against your account by payees who are non-customers
- Maximum Dollar Check Cashing Limit: Teller line protection that prevents checks above your established threshold, from being cashed at the bank by non-customers

Benefits

- No monitoring required by you

Considerations

- Applies to teller line cashing for non-customers only
- Use only with business accounts dedicated to electronic payment

ACH fraud goes mainstream

Relative to check fraud, ACH fraud remains rare today

Twenty three percent of organizations reported fraud attempts in 2011

HOWEVER, times are changing. As ACH use broadens, ACH fraud schemes grow. On the list:

Account Hijacking
Fraudsters use compromised customer credentials to hijack the origination system and use it in the legitimate account holder's name.

Identity Fraud
Criminals create false identities, social engineer their way into obtaining ACH origination capabilities and then initiate fraudulent debits.

ACH Kiting
A version of check kiting with a cyber twist, ACH kiting involves a pair of accounts used for fraudulent purposes — an ACH debit is originated from one account and drawn on the other; the available balance is taken out before settlement.

Reverse Phishing
Instead of e-mails attempting to fraudulently obtain corporate banking information, perpetrators send e-mails to corporates that provide fraudulent banking information, redirecting ACH payments to an account they control.

Insider Origination Fraud
Insiders at a merchant or bank manipulate an ACH origination file to skim funds from a company.

Counterfeiting
ACH debits generated through the electronic conversion of a counterfeit check.

ACH best practice – debit block

How it works

- Blocks ACH debits from posting based on criteria selected by you

Benefits

- ACH debits are automatically returned based on your instructions
- Examples of instructions
  - Block all ACH Debits
  - Block all ACH Debits for amounts greater than $X,XXX
  - Block all ACH Debits from companies other than X corporation, Y corporation, and Z corporation.
- No monitoring required by you

Considerations

- Separate accounts required for check writing and electronic payments (ACH, wires)
- Debits not affected by blocking:
  - ACH debits that offset ACH credit entries originated by you
  - Reversals of previously received ACH credit entries (as defined by NACHA)
  - Reclamation entries
  - Debits to accounts initiated by Bank to correct processing errors, effect back-valuations or make other adjustments

ACH best practice – transaction review

How it works

- Allows clients to review and decision ACH transactions that posted to their account the prior day

Benefits

- Clients can limit the items to review through the following filters
  - Debit and or Credit transaction
  - Dollar Amount
  - Transaction Type
  - Originating Company ID/Name
- Timely return of unauthorized ACH transactions
- Visibility into the all ACH activity matching filter criteria
- Ability to make pay/return decisions for each item matching filter criteria

Payables fraud prevention – *internal best practices*

Segregate Accounts

- Account Type: Deposits or Disbursements
- Payment Method: Check, ACH, Wire
- Payment Type: Payroll, Claims
- Payment Amount/Volume: High or low

Segregate Duties:

- Checks – Originate payment, Submit Issuance, Decision Exceptions
- Wires - Creating, Approving, Releasing Wires

Dual Approval:

- Require dual approval at critical checkpoints such as approving wires or approving Positive Pay exception decisions
- Monitor and reconcile accounts daily

Payables Fraud Prevention – Online Security

- Mask account numbers and Tax ID numbers in your correspondence
- Use encrypted email for confidential, non-public information
- Ensure SecureID® tokens are collected and passwords are changed when an employee leaves the company
- HR Policy – Forced vacations and job rotations
- Utilize file encryption techniques — encryption is the process of transforming information (referred to as plain text) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge (usually referred to as a key)
- Multi-factor-based individual and machine authentication models: require an additional type of authentication, such as something you know (for instance, a password or PIN) and something you have (such as a piece of hardware or software that uniquely identifies the individual)

Assessment

Example Municipality*

- Utilize an On-Line Treasury Workstation
- No business need to allow their payees to cash checks at branches

Account	Account Type	Monthly Activity	Recommended Solutions
XXXXXX8765	Check: AP, Misc. Vendors	1,200 Checks	
XXXXXX8768	ACH: AP, Payroll through ADP	4 ACH Debits	
XXXXXX8770	Deposit: AR, Client Receipts	75 Deposits	
XXXXXX8772	ACH: Vendor Payments & Refunds	65 ACH Debits 7 ACH Credits	
XXXXXX8774	Check: Misc. Payable	150 Checks	

*Fictitious client created for purposes of this case study

Chase Solutions

Segregate Accounts By: Purpose, Volume, and Payment Channel

Allows you to: Comprehensively protect accounts

Account	Account Type	Monthly Activity	Recommended Solutions
XXXXXX8765	Check: AP, Misc. Vendors	1,200 Checks	Positive Pay with Payee Name Verification No Check Cashing, ACH Debit Block – All
XXXXXX8768	ACH: AP, Payroll through ADP	4 ACH Debits	ACH Debit Block – Exclude all but ADP Post No Checks
XXXXXX8770	Deposit: AR, Client Receipts	75 Deposits	ACH Debit Block – All Post No Checks
XXXXXX8772	ACH: Vendor Payments & Refunds	65 ACH Debits 7 ACH Credits	ACH Transaction Review Post No Checks
XXXXXX8774	Check: Misc. Payable	150 Checks	Reverse Positive Pay No Check Cashing, ACH Debit Block – All