J.P.Morgan

NOT-FOR-PROFIT BANKING

Mitigating Payments Fraud Risk:

Strategies and Best Practices for Not-For-Profit Organizations

Payments fraud is an equal opportunity offender and the not-for-profit sector is not immune. As charitable organizations pursue quality benefits and services to their members and beneficiaries in an environment of constrained budgets and regulatory pressures, they cannot afford the exposure to potential financial loss. All payment methods – checks, ACH and commercial cards – are vulnerable. To protect against this crime, every operating account should have some measure of fraud prevention in place to avoid being compromised.

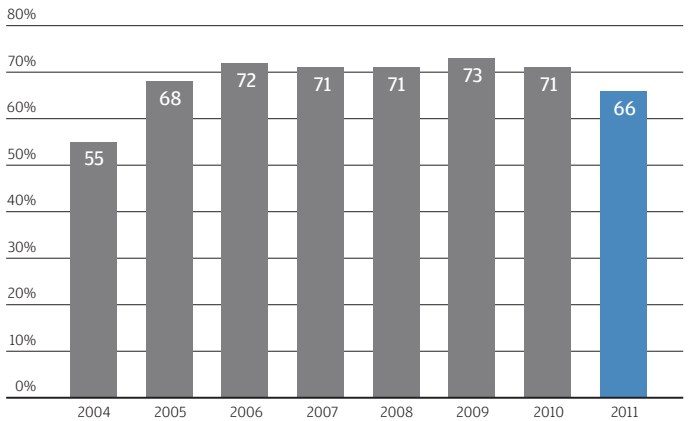
This white paper – prepared especially for financial and treasury officers operating in the not-for-profit marketplace – will provide strategies and best practices to help organizations protect against the risks and potential financial loss resulting from payments fraud.

A Lack of Vigilance is the Fraudster's Workshop

Despite inching back from its peak in 2009, the incidence of payments fraud remains widespread according to the Association for Financial Professionals (AFP). Results[1] from responders to the 2012 AFP Payments Fraud and Controls Survey revealed that:

- Two thirds of organizations experienced attempted or actual payments fraud in 2011.
- 74 percent suffered no financial loss having deployed sound fraud mitigation policies.
- Incidents of fraud increased for 28 percent of respondents in 2011 over 2010.

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



Source: 2012 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2012. Underwritten by J.P.Morgan. Page 4.

Schemes and Scams: How the Perpetrators Practice Their Craft

Sophisticated fraudsters and scam artists operate in a technology-enabled, target-rich environment. Easy access to PCs, scanners, off-the-shelf software and malware enable them to probe for weaknesses in account security and the absence of anti-fraud countermeasures as they seek out their victims. To defeat them, not-for-profit organizations must know where they are vulnerable and the various schemes that criminals might use to strike them:

Check fraud: "Checks continue to be the most popular target for criminals committing payments fraud. This is remarkable given the precipitous decline in corporate use of checks in recent years."[2] Despite the drop in check usage as a percentage of total payments, checks still represent large dollar transactions. As an easy-to-commit, technology enabled crime check fraud makes settling transactions with checks a risky proposition. Common methods of check fraud include payee name alteration, forged signatures and counterfeiting. Check kiting is another. In this scenario, a person deposits a non-sufficient fund check into an account, and then writes another check against that amount for another account.

Email schemes: Phishing is a common technique used to ensure bigger paydays by fraudulently hooking and using a charitable organization's proprietary financial information. Phishing emails may contain links to bogus websites or ask for financial information using clever or compelling language, such as an urgent need to update account data, decline a payment or ensure operating account security.

ACH fraud: As more not-for-profits electronify their payables, the incidence of ACH scams is increasing. Accounts are being accessed for unauthorized ACH payments through methods that include account hijacking, ACH kiting and identity fraud. Reverse phishing is another scheme that should be on the radar. Instead of sending emails attempting to falsely obtain the organization's information, fraudsters send not-for-profits emails containing fraudulent banking information that redirects ACH payments to an account they control.

[1] 2012 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2012. Underwritten by J.P.Morgan.
[2] Ibid.

Mobile: The RSA Monthly Online Fraud Report for January 2011 revealed a 27 percent increase in phishing attacks in 2010 over 2009, as phishing evolved in sophistication and began to attack new channels such as mobile phones. The technologies that enable quicker availability of funds through mobile deposits are increasing both opportunities to strike and the odds of scammers defeating the system. This is prevalent in the mobile communication marketplace as a recent study shows that "mobile users are three times more likely than a desktop user to enter their personal information to a phishing site."[3]

Commercial Cards: As the preferred tool for managing procurement and travel spend across the procure-to-pay cycle while complying with audit and regulatory guidelines, commercial cards are proliferating. The increased usage - especially among purchasing cards that account for 75 percent of all business-to-business payments - creates more opportunities for outside entities and employees to defraud their organizations. One common scheme is through third party merchant/merchant processors where card data is compromised and unauthorized individuals could potentially utilize the account information for their benefit.

Fighting Back: Tactics, Strategies and Best Practices

Comprehensive planning, controls and oversight - aligned with prudent risk management - are essential tools for developing a payments fraud deterrence playbook. Starting from the premise that the best offense is a good defense, financial decision-makers in the not-for-profit sector can access a set of tactical initiatives and strategic solutions - from choosing paper stock to deploying leading-edge products - that integrate seamlessly with their payments fraud prevention plan.

Tactical Initiatives

Paper: In addition to transitioning from paper checks to electronic payments, many philanthropic organizations are are implementing practical measures internally to defend against any potential loss from check fraud by:

- Using 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, and more.
- Purchasing stock from reputable merchants that they know.
- Securely storing check stock, deposit slips, bank statements and canceled checks.
- Implementing secure financial document destruction processes.
- Establishing an employee order and reorder policy for check stock.
- Initiating dual controls over check stock, check issuance and account reconciliation.

Electronic: Converting paper-based payments to electronic delivery whenever possible is a strong deterrent to check fraud. Looking beyond the use of online banking channels for treasury management, not-for-profits are evaluating other defensive measures:

- Conduct a thorough vetting of all suppliers as many not-for-profit decision-makers believe that the perpetrators are above board.
- Mask account numbers and tax ID numbers in your correspondence.
- Use encrypted email for confidential, non-public information.
- Ensure that passwords are changed when an employee leaves your organization.

PREVALENCE OF FRAUD BY PAYMENT METHOD

(Percent of Organizations Subject to Attempted or Actual Payments Fraud in 2011)

	All respondents	Revenues under $1 billion	Revenues over $1 billion	Revenues over $1 billion < 26 payment accounts	Revenues over $1 billion > 100 payment accounts	Majority of transactions within the U.S.	Significant percentage of non-U.S. transactions
Checks	85%	82%	90%	92%	90%	88%	64%
ACH debits	23	27	22	20	31	27	22
Corporate/commercial purchasing cards	20	22	20	21	13	19	21
Consumer/small business credit or debit cards (accepting for payments)	12	13	11	12	12	11	13
ACH credits	5	4	5	3	8	3	4
Wire transfers	5	4	4	1	8	3	4
Payroll and other benefit cards	5	4	6	7	5	8	3

Source: 2012 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2012. Underwritten by J.P.Morgan. Page 5.

[3] Mobile Users More Vulnerable to Phishing Attacks. Help-Net Security, January 4, 2011.

Internal Controls: Segregating accounts for different payment vehicles or purposes allows for timely and focused review of all payment activity. Other methods include:

- Segregating and defining duties: making payments vs. reconciling accounts.
- Consolidating operating accounts and eliminating inactive ones.
- Mandating dual approval at vulnerable touch points such as creating, approving and releasing wires, and approving Positive Pay exception decisions.
- Monitoring accounts regularly and increasing the frequency of reconciliation, i.e., daily.
- Using online statements, reporting, and reconciling services to accelerate the process.

Online Security: Masking account numbers and Tax ID numbers in all correspondence and using encrypted email for confidential, non-public information protects accounts from being hijacked. Additional fraud prevention measures include:

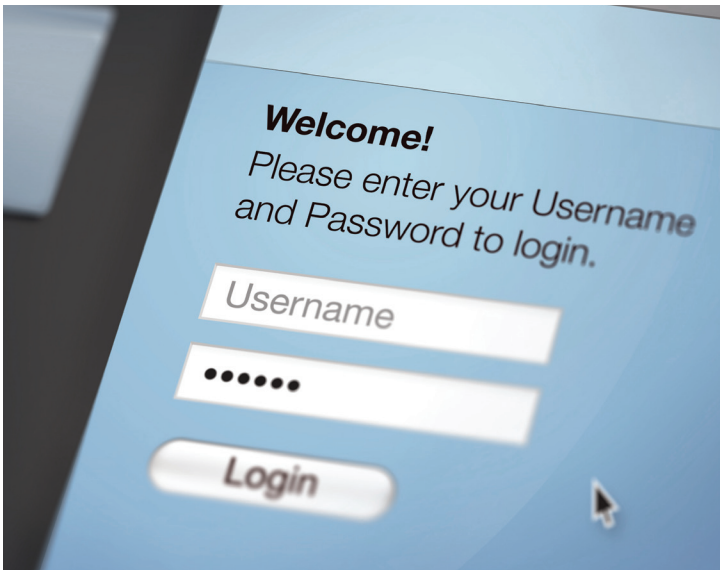
- Building awareness of the latest fraud trends within your organization such as spear phishing and malware so staff will not be mislead into providing sensitive information or unknowingly download malicious software from phony websites.
- Relying on a trusted financial partner for:
  - Comprehensive fraud monitoring and detection systems
  - State-of-the-art encryption techniques
  - Enforcement of dual-authority or "step-up authentication" for transactions

Strategic Product Initiatives

Organizations are best served when they combine the features and functionality of leading-edge products with the expertise of a strong financial partner with demonstrated success working in the not-for-profit sector. That relationship is the gateway to a suite of fraud mitigation solutions to protect and secure proprietary data integrity:

Positive Pay: Electronically matches all checks presented for settlement with all checks issued by the user, including account number, serial number and dollar amount. When bundled with the Payee Name Verification, Positive Pay becomes more robust enabling verification of payee name on the check with the payee name provided on the issue file by the user. In addition, Positive Pay:

- Provides next-day ability to monitor and control checks presented against an account so only authorized items are paid.
- Generates daily email notification of exceptions enabling users to perform the decisioning function.
- Offers teller-line protection as a standard feature.
- Is the number one solution for combating check fraud.



Reverse Positive Pay: Presents check images to users who control the matching of checks presented to checks issued so that only authorized items are paid. In addition to flexible viewing options, users can establish dollar limits so checks below the set amount are paid without the need to review. When evaluating Reverse Positive Pay, a number of factors should be considered:

- Solution should be used only with business check writing accounts.
- Daily involvement is required to make decisions on exceptions.
- Users are responsible for matching checks presented to checks issued.
- Both teller-line and payee verification services are available as non-standard offerings.

ACH Debit Block: Enables charitable organizations to specify which companies are and are not authorized to post ACH debits to their accounts, automatically blocking those that are not authorized. ACH Debit Block uses systems technology to immediately compare incoming ACH debits against a range of user-defined criteria, including:

- Solution should be used only with business check writing accounts.
- Daily involvement is required to make decisions on exceptions.
- Users are responsible for matching checks presented to checks issued.
- Both teller-line and payee verification services are available as non-standard offerings.

To post successfully, checkpoints must match exactly or the unauthorized transactions are rejected. While no monitoring is required on the part of the user, separate accounts are required for check writing and electronic (ACH and wire) payments.

ACH Transaction Review: Allows not-for-profit financial decision-makers to define the processing rules. Users can review, confirm and render decisions on whether ACH transactions that posted to their account the prior day are authorized or not on a case-by-case basis. Transactions that require review can be filtered by any combination of debits and credits, organization IDs, dollar amount/range and transaction type. Engaging ACH Transaction Review enables users to leverage:

- Timely return of unauthorized ACH transactions.
- Increased visibility into ACH activity.
- Expedited pay/return decision-making for each item matching their filter criteria.

Check Print Outsourcing: The ability to assign the check print function to a specialized third party that might include an organization's banking partner represents a major leap forward in adding controls to prevent check fraud.

The value-add, beyond providing checks designed with all the requisite anti-fraud measures, is the ability to accept integrated payment data files to consolidate and process payments. Using this method, a not-for-profit organization sends a single file with instructions for wire transfers, checks, ACH and card transactions. The file is authenticated, contents validated, encrypted for secure transmission, and then routed over the appropriate settlement channel cost-effectively. Upgrading the level of protection against check fraud across the procure-to-pay cycle is not the only benefit. Outsourcing check print helps reduce operating expenses, eliminates reliance on paper-based processes and improves workflow efficiencies.

The growing risk of payments fraud, the potential financial loss, and the increasing sophistication of the perpetrators is influencing decisionmakers to re-define financial risk management within the not-for-profit sector and seek solutions. For more information, please contact your J.P. Morgan Not-For-Profit Banking representative or visit JPMorgan.com/commercialbanking.

For more information, please contact your Not-For-Profit Banking representative or visit JPMorgan.com/commercialbanking

WP_12_010