A CHASE THOUGHT LEADERSHIP INITIATIVE

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE...
FRAUD RISK PROTECTION STRATEGIES FOR BUSINESS

CONTENT SNAPSHOT

What You'll Learn Inside:

- Making the Case for Prevention
- Scams and Schemes: How the Game is Played
- Best Practices for Taking the Offensive
- Tactical Initiatives/Strategic Solutions

CHASE

FRAUDSTERS DO NOT DISCRIMINATE

Business fraud – whether initiated externally by cyber criminals or internally by employees behaving badly – is widespread, and the fraudsters who practice it are equal opportunity offenders. No business – regardless of type or size – is immune, and most cannot afford the exposure to potential financial loss. Every payment method – from checks to ACH to commercial cards – is vulnerable.

Commonly understood as dishonesty calculated for advantage, fraud is a deliberate misrepresentation that causes a person or business to suffer damages, often in the form of monetary losses, through deception or concealment. Fraudulent acts can be committed through media channels that include mail, wire, phone, and the Internet. From identity theft, check fraud and e-mail scams to cyber crime, padded expense reports and manipulated financial statements – the range of possible schemes is extensive.

Paper checks continue to be the payment method most vulnerable to fraud attacks.

Recent research indicates that anti-fraud controls tend to lag at smaller organizations. The vacuum caused by this lack of oversight creates a fraudster's paradise. To mount an effective defense, all operating accounts and business processes involving company funds should have some degree of fraud protection in place to avoid being compromised.

This white paper provides a suite of prevention strategies, tactics and best practices to help businesses of all sizes reduce both the financial and reputational risks associated with fraud.

MAKING THE CASE FOR PREVENTION

Despite having receded from its 2009 peak, payments fraud remains prevalent, according to the Association for Financial Professionals (AFP). Results[1] from the 2013 AFP Payments Fraud and Control Survey revealed that:

- 61 percent of participants experienced attempted or actual payments fraud in 2012.
- 27 percent of respondents reported that incidents of fraud increased in 2012 over 2011.
- Among organizations suffering a financial hit, the typical loss was $20,300.
- 73 percent suffered no financial loss, having deployed sound fraud mitigation policies.

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 & with <26 Payment Accounts	Revenues Over $1 billion & with >100 Payment Accounts	Majority of Transactions with the U.S.	Significant Percentage of Non-U.S. Transactions
Checks						
87%	87%	91%	93%	94%	92%	87%
Corporate/Commercial						
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

Source: 2013 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2013. Underwritten by J.P. Morgan.

1. 2013 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2013. Underwritten by J.P. Morgan.

Paper checks continue to be the payment method most vulnerable to fraud attacks, according to the AFP survey, with 87 percent of organizations affected having reported that their checks were targeted. Among respondent companies victimized by at least one attempt of check fraud in 2011, 16 percent suffered a financial loss while a small percentage of organizations that convert checks electronically indicated that their check conversion service was used to commit fraud.

Not all fraud attempts originate outside company walls. Occupational (workplace) fraud is a significant threat as well. The Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study published by the Association of Certified Fraud Examiners (ACFE) revealed that companies with <100 employees and those with 100-999 employees tend to be more at risk as they often have limited resources and fewer anti-fraud prevention tools in place. Results[2] from the ACFE report confirm that:

- Only 56 percent of organizations with <100 employees underwent external audits of their financial statements, compared with 91 percent of businesses with 100 or more employees.
- Employees received fraud training at just 18.5 percent of small organizations compared with almost six in 10 larger organizations.
- Management certification of financial statements occurred at 43 percent of small organizations compared with 81 percent of larger ones.

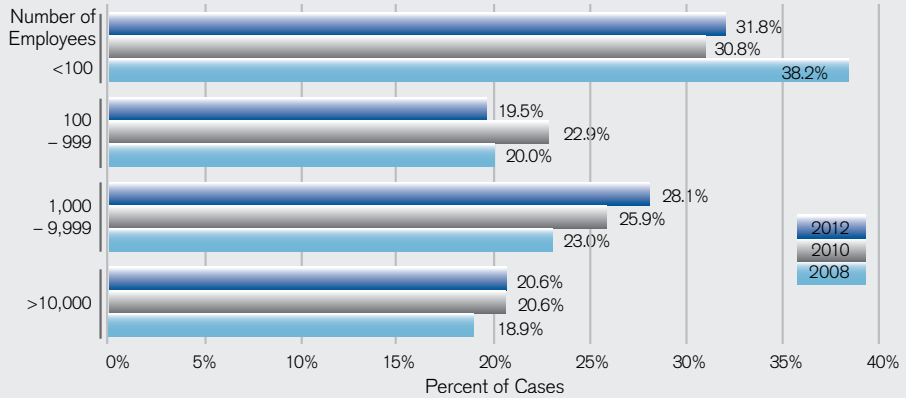
The fallout from fraud extends well beyond financial loss by placing an organization's reputation at risk too.

Once victimized and without a sufficient array of fraud prevention and training strategies in place, the odds of recovering losses become longer as nearly half of all organizations victimized by business fraud never see any of their lost revenue.

The fallout, however, extends well beyond financial loss by concurrently placing an organization's reputation at risk. Reputational risk represents the potential that any negative publicity involving a company's business practices, whether true or not, will not only damage third-party credibility, but drive customers away, result in revenue loss and require costly litigation.

Fraud prevention has become serious business, and organizations should do all that is reasonable to increase their level of protection and avoid becoming a victim.

Size of Victim Organization – Median Loss



Source: Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study published by the Association of Certified Fraud Examiners (ACFE).

2. Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study published by the Association of Certified Fraud Examiners (ACFE), 2012.

SCAMS AND SCHEMES: HOW THE GAME IS PLAYED

Highly sophisticated, tech-savvy and determined, fraudsters function in a target-rich and technology-enabled environment. Easy access to PCs, scanners, off-the-shelf software and malware enable them to probe for weaknesses in account security as they seek out their victims. To defeat them, organizations must know where they are vulnerable and be able to identify the various scams and schemes that criminals might use to strike their operation:

- Check Fraud: "Checks continue to be the most popular target for criminals. This is remarkable given the precipitous decline in corporate use of checks in recent years."[3] Despite the drop in check usage as a percentage of total payments, checks still represent large-dollar transactions, making settlement with checks a risky proposition. Common methods include payee name alteration, forged signatures and counterfeiting. Check kiting is another, whereby a person deposits a non-sufficient fund check into an account, and then writes another check against that amount for another account.

As organizations become more successful at monitoring for phishing attacks, two other threats – "vishing" and "smishing" – are increasing.

- Phishing is a common technique used to ensure bigger paydays by fraudulently hooking and using an organization's proprietary financial information. Phishing e-mails 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.
- Spear Phishing targets employees or high-profile individuals within an organization in order to obtain sensitive information or get the victim to click on a link or attachment that carries malicious software. Once the malware is installed, anything the user types on the computer can be accessed, including corporate credentials.
- Vishing is used to gain unauthorized access to personal and financial information. Typically, a "war dialer" is used to call thousands of phone numbers. Automated recordings tell consumers that suspicious activity has been detected on their credit cards or bank accounts and instruct them to contact their bank. Unsuspecting individuals comply, giving out personal data through a false phone number.
- Smishing is a Short Message Service phishing attack whereby fraudsters send a text message to an individual's mobile phone asking the target to call a false phone number or visit a look-alike website to confirm personal data.

Nearly 50 percent of organizations never recover losses suffered due to fraud.

August 2012 saw the FBI issue an alert for a Ransomware application known as Reveton. Designed to extort money, victims are lured to a download website where the application is installed on the user's PC, causing it to freeze. A screen then appears warning that the user has violated federal law and that their IP address was identified by the FBI as having visited websites that feature child pornography and other illegal content. The user is instructed to pay a fine to the U.S. Department of Justice using a prepaid money card service in order to unlock their PC. After the "ransom" is paid, the screen is generally removed, but the malware may continue to operate on the compromised computer.

ACH Fraud: As more organizations electronify their payables, the incidence of ACH scams is increasing. Accounts are being accessed for unauthorized ACH payments through a number of schemes that industry experts have identified and should be on the radar. These include:

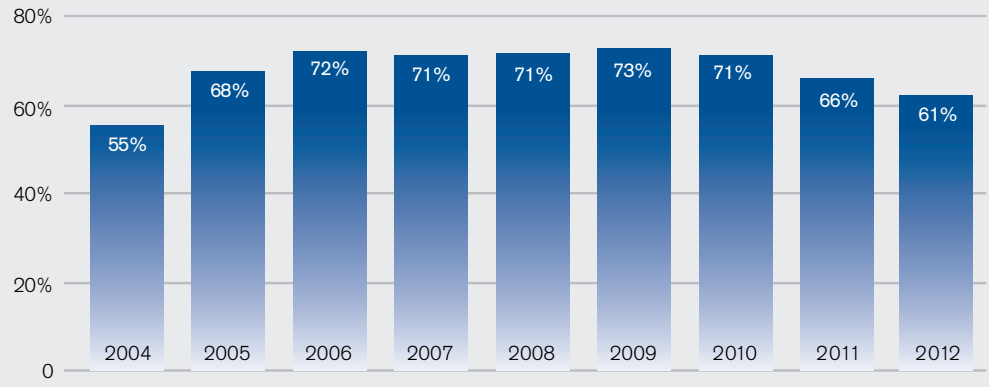
- Reverse Phishing: Instead of sending e-mails attempting to falsely obtain corporate banking information, fraudsters send corporations e-mails containing fraudulent banking information that redirects ACH payments to an account they control.

3. Ibid. 1.

- Account Hijacking: Fraudsters use compromised customer credentials that might, for example, be accessed by invading an employee's laptop, to hijack the origination system and use it in the legitimate account holder's name, quickly withdrawing funds before the fraud is discovered.
- Identity Fraud: By creating false identities, criminals social engineer their way into obtaining ACH origination capabilities and then initiate fraudulent debits.
- ACH Kiting: A cyber version of check kiting that capitalizes on the short ACH window of funds movement and availability and uses a pair of accounts. An ACH debit is originated from one account and drawn on the other, with the available balance taken out before settlement.
- Insider Origination Fraud: Involves insiders at a merchant or bank who manipulate ACH origination files to skim funds from a company, and Counterfeiting that generates ACH debits through the electronic conversion of a counterfeit check.

As more organizations electronify their payables, the incidence of ACH scams is increasing.

Percent of Organizations Subject to Attempted or Actual Payments Fraud



Source: 2013 AFP Payments Fraud and Control Survey Report of Survey Results, Association for Financial Professionals, March 2013. Underwritten by J.P.Morgan.

Mobile: 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."[4]

There are two new Trojan attacks (applications that appear innocuous but use embedded malicious code to perform fraudulent tasks) affecting mobile devices that run the Android operating system. Trojans enable mobile devices to be remotely controlled and create serious risks for personal information stored on compromised Android devices. Because these applications operate in an open environment, they are virtually impossible to control:

- Loozfon: An information-stealing piece of malware used by criminals to lure victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out e-mail. A link within these advertisements leads to a website designed to push Loozfon on the user's device to steal contact details from the user's address book and the infected device's phone number.
- FinFisher: A form of Spyware capable of taking over the components of a mobile device. When installed, the mobile device can be controlled and monitored remotely no matter where the target is located. FinFisher can be easily transmitted to a smartphone when the user visits a specific web link or opens a text message masquerading as a system update.

4. Mobile Users More Vulnerable to Phishing Attacks. Help Net Security, January 4, 2011.

Commercial Cards: As the preferred tool for managing procurement and travel spend, usage is increasing – especially among purchasing cards that account for 75 percent of all business-to-business payments. This growth is creating more opportunities for outside entities and employees to defraud their organizations.

BEST PRACTICES FOR TAKING THE OFFENSIVE

Sound planning, controls and oversight – integrated with prudent risk management – are essential tools for developing a fraud deterrence program. At a minimum, organizations should begin by creating an environment governed by honesty and integrity, and:

- Assess scams and schemes that present the greatest threats and match up affordable countermeasures.
- Train managers and employees to recognize behavioral characteristics that might be early warning signs of potential fraud, such as someone living beyond his/her means.
- Set up a confidential hotline for employees to safely report incidents of fraudulent practices.
- Maintain security protocols as basic as ensuring computer passwords are unique and complex.
- Conduct secure transactions using approved methods, and be careful when sending sensitive information over unsecured lines, e-mails and websites.
- Regularly review credit reports and financial statements for any suspicious or unauthorized credit accounts and make use of electronic alerts and notifications for extra protection.

Converting paper-based payments to electronic delivery is a strong deterrent to fraud.

TACTICAL INITIATIVES

Paper: While transitioning from paper checks to electronic payments, use high-quality check stock with built-in security features. These include fluorescent fibers, watermarks, chemical resistance, bleach-reactive stains, thermo-chromatic ink, endorsement backer and micro printing. Purchasing stock from reputable merchants, storing check stock, deposit slips, bank statements and canceled checks securely, and implementing secure financial document destruction processes are additional steps to take.

Electronic: Converting paper-based payments to electronic delivery is a strong deterrent to fraud. Business owners are evaluating other defensive measures that include scrutinizing vendors, as many decisionmakers believe the perpetrators are above board, masking account numbers and tax ID numbers in correspondence and using encrypted e-mail for confidential, non-public information.

Internal Controls: Segregating accounts for different payment vehicles or purposes allows for timely and transparent review of all payment activity. Other methods include separating and defining responsibilities such as making payments vs. reconciling accounts, consolidating multiple operating accounts and eliminating inactive ones, mandating dual approval at vulnerable touch points like creating, approving and releasing wires, and approving Positive Pay exception decisions.

Online Security: Using encrypted e-mail for confidential, non-public information protects accounts from being hijacked. For additional security, steps can be taken to build awareness of the latest fraud trends within your organization so staff will not be duped into providing sensitive information or unknowingly download malicious software. Another prudent decision is to rely on a trusted financial partner for comprehensive fraud monitoring and detection systems, state-of-the-art encryption techniques and enforcement of dual-authority or “step-up authentication” for transactions.

STRATEGIC SOLUTIONS – DOING OUR PART

Organizations are best served when they combine the features and functionality of best-in-class products with the expertise of a strong financial partner with success working across all business sectors. That relationship is the gateway to a suite of fraud protection solutions that can help secure the integrity of proprietary financial data:

Best suited for businesses with volume of >200 checks per month, Positive Pay is the number one solution for combating check fraud.

Positive Pay: The number one solution for combating check fraud, fee-based Positive Pay is designed for businesses that want Chase to help monitor their commercial transactions against suspicious check activity. 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 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. Best suited for businesses with volume of >200 checks per month, Positive Pay enables you to enter information about checks written on Chase.com. All checks presented for payment are compared against the details provided and when checks presented for payment don't match, unauthorized checks are displayed as exceptions. You review check exception images online and decide which checks we should pay or return. Any checks not reviewed by the decision cut-off time will be returned and a fee charged for each returned item.

Reverse Positive Pay: Created for organizations that want to monitor check activity on their own, this free solution enables businesses to engage Chase to provide the necessary tools, functionality and support. Recommended for organizations with a volume of >50 but <200 checks per month, Reverse Positive Pay delivers 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 set a dollar amount threshold so all checks below the set amount are paid without the need to review.

Keep the following in mind when evaluating Reverse Positive Pay. Its use should be for business check writing accounts only, daily involvement is required to make decisions on exceptions, and users are responsible for matching checks presented to checks issued.

Electronic alerts provide an extra layer of account security and help monitor balances, large transactions and account activity.

Electronic Alerts: These updates can be personalized for any Chase Business checking, savings, credit card, line of credit, and loan account and received at any e-mail address, any phone number or via text message. Two types of alerts are offered based on specific needs:

- Security Alerts: You can set dollar limits for different transactions, i.e., ATM withdrawals, debit card activity, money transfers and online bill payments. Chase will contact you when your debit card transactions or ATM withdrawals exceed specific limits and/or an automatic payroll or bill payment exceeds a specific limit.
- Daily Alerts monitor your account activity and transactions. Choose the alerts you want, set your trigger amounts, and we'll notify you by e-mail or phone to help you monitor balances, large transactions and account activity.

Paperless Statements: Free up your business from receiving and storing mailed statements. Electronic statements improve security by reducing the risk of a statement getting lost or stolen, allow you to review and print up to seven years of statements anytime, accelerate data access and eliminate snail mail. You'll be notified by e-mail when your statement is ready.

ACH Debit Block: Enables you to specify which companies are and are not authorized to post ACH debits to their accounts, automatically blocking those that are not approved. ACH Debit Block uses systems technology to immediately compare incoming ACH debits against a range of user-defined criteria, including account number, transaction code, check amount (dollar amount

ceilings can be applied), effective date and identity of company sending the check. 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 users to review, confirm and render decisions on whether 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, company IDs, dollar amount/range and transaction type. Engaging ACH Transaction Review enables users to return their unauthorized ACH transactions on a timely basis, increase the visibility into ACH activity, and expedite pay/return decisionmaking for each item matching their filter criteria.

"Technology breeds crime. What I did 35 years ago is 2,000 times easier today."

– Frank Abagnale

The growing threat of business fraud has more organizations re-examining their fraud protection policies. While fraudsters have displayed sophistication and determination in designing their plans of attack, the banking industry has worked diligently to adopt and deploy tough anti-fraud solutions to defeat them.

For insight and perspective on how to create an effective fraud protection strategy, speak with your Chase Banker. Learn how Positive Pay, Reverse Positive Pay, Paperless Statements, Account Alerts and other Chase anti-fraud countermeasures can be seamlessly integrated with your operating accounts to help mitigate the risk and potential financial loss associated with fraud.

We offer a wide range of credit and cash management services, merchant services, business checking products, and other financial tools and resources that can help your business access working capital, improve cash flow and compete for business more effectively.

Chase business customers can also access an exclusive series of webinars and live, high-powered business events. All are designed to provide timely and relevant information and ideas for business owners looking to move their companies forward while giving them the opportunity to meet and network with experts and other business owners.

For more information, please contact a Chase Cash Management Solutions Specialist at **877-212-2741**.

The following resources offer valuable insight on fraud prevention, detection and deterrence:

- The Association of Certified Fraud Examiners (ACFE): www.acfe.com
- Association for Financial Professionals: www.afponline.org
- Internet Crime Complaint Center (IC3): www.ic3.gov
- National Check Fraud Center: www.ckfraud.org
- National Automated Clearinghouse Association (NACHA): www.nacha.org
- The Better Business Bureau: www.bbb.org/us
- The Internal Revenue Service: www.irs.gov/uac/Suspicious-e-Mails-and-Identity-Theft
- The Department of Justice: www.justice.gov/criminal/cybercrime/documents.html
- Frank Abagnale, recognized expert on fraud, forgery and embezzlement: www.abagnale.com

CHASE