treasuryXpress
Smart. Scalable. On-Demand.

UNDERSTANDING PAYMENT FRAUD TO PREVENT ATTACKS

ABSTRACT

Payment crime has grown into a rampant threat for treasuries of all sizes. Perpetrators of payment crime have grown more sophisticated and capable than ever before. Accordingly, countless treasury teams across the globe are struggling to acquire and implement immediate payment protection capabilities.

The key to successful payment protection lies in understanding the points of vulnerability within your organization that are likely to be targeted for attack, and implementing a proactive defense against such attacks.

EXECUTIVE SUMMARY

Payment crime has grown into a rampant threat for treasuries of all sizes. Perpetrators of payment crime have grown more sophisticated and capable than ever before, leveraging knowledge of the common points of vulnerability that leave most treasury organizations and payment operations exposed to risk. Accordingly, countless treasury teams across the globe are struggling to acquire and implement immediate payment protection capabilities.

And yet, the goal of implementing effective and comprehensive payment protection solutions can be easily achieved. In spite of the escalating risk that treasury organizations face, fighting payment fraud and enhancing security protocols do not have to be daunting challenges.

The key to successful payment protection lies in understanding the points of vulnerability within your organization that are likely to be targeted for attack, and implementing a proactive defense against such attacks. It's also important to understand that help is at hand; no organization -- whether large or small -- must face the escalating onslaught of payment crime alone.

This white paper will spotlight the growing risk faced by organizations worldwide in five key areas of vulnerability, and provide a how-to overview for implementing appropriate best-practice payment security protocols.

No Time for Complacency

We are living in dangerous times. Unfortunately, that's a statement that applies to many aspects of life. But it's particularly applicable to corporate treasury professionals. Criminals seem to be doubling-down on their efforts to perpetrate fraud, leveraging the tools of modern technology to great effect.

TreasuryXpress recently conducted a poll amongst 200+ global treasury participants. The results of which emphasized the urgency of the problem. The survey revealed that 63% of respondents had suffered a payment fraud attack within the previous 12 months, with 51% of companies reporting that at least one attack had occurred in just the previous 6 months. The poll also found that the most common types of fraud attacks were as follows:

- File transfer - 4%
- Employee exits - 9%
- Social engineering - 31%
- Fraudulent messages - 43%

The 2016 Global Treasury Fraud & Controls Survey produced by Strategic Treasurer and Bottomline Technologies sheds even more light on just how serious the problem has become. The survey found that fraud payoff is more lucrative than ever for criminals that target companies that are ill prepared to deal with the onslaught of fraud attempts. Consider the following typical payout ranges for common forms of fraud, as revealed by the survey:

- System Fraud: Typical payout range of $1 million to $10 million per occurrence
- Wire Fraud: Typical payout range of $130,000+ per occurrence
- Check Fraud: Typical payout range of $1,000 to $2,000 per occurrence

The survey also revealed that though all forms of financial fraud are on the rise, "…traditional check forgeries remain on top of the list of attempts." Wire/imposter fraud, ACH fraud, and check conversion fraud complete the list of the top four types of fraud attempts. In summation, the survey report notes that "On the whole there has been a progressive increase in both fraud attempts and successes on multiple fronts."

One additional fact revealed by the survey was rather startling: "Fifty-seven percent of more than 300 respondents…say they have no formal framework in place to protect their organizations from payment fraud." With per-incident fraud payouts better than ever and a large flock of complacent sheep waiting to be sheared, it's no wonder that fraud perpetrators are enjoying unprecedented profits!

Don't Underestimate Your Enemy

"Know thine enemy." That ancient quote, or various versions thereof, has been attributed to many sources, including Sun Tzu's Art of War. Regardless of who first offered that advice, it's timeless. And it certainly applies to the 'art' of payment fraud prevention. Treasurers tasked with protecting their organizations from fraud would be well advised to know their enemy, because the enemy is quite formidable.

Though the common criminal may be perceived as somewhat of an incompetent dullard, that description certainly does not apply to the successful perpetrators of fraud. When it comes to perpetrating payment fraud, criminals' ability to practice their craft often outstrips their target victims' abilities to protect themselves.

And this class of criminal tends to be quite technologically sophisticated and creative, focusing frequently on some form of cyber-attack. There are, in fact, five main points of attack that cyber-criminals tend to focus upon:

1. Social Engineering Attacks: These attacks are typically perpetrated from within a company, with internal operatives (employees) working to aid an outside entity in breaking through security protocols. Notable examples of points-of-weakness that increase vulnerability to social engineering attacks include:
    - Communicating passwords between coworkers
    - Systemic tolerance of weak passwords
    - Accepting emails
    - Downloading unknown links that prompt for password change

2. Fraudulent User Messages: Criminals will often submit fraudulent messages by impersonating legitimate users. This frequently happens when they have already processed payments to a bank, either through legitimate means or via a back door.

3. Weak File Transfer Protocols: Attackers who have acquired information that reveals an insecure file protocol can use that information to hack into an account and submit their own files.

4. Employee Exit Protocols: Disgruntled employees often have access to accounts that present them with the opportunity to commit fraud before their access is terminated. At medium to large companies, particularly, there's often a considerable delay in terminating sign-in access for exiting employees. The problem is likely to be exacerbated with employees that have been granted access to multiple payment platforms.

5. Lenient Payment Workflows: In many organizations, the desire for convenience results in payment workflows that tend to be more lenient and less secure.

Putting Security Protocols in Place

Protecting your organization from payment fraud should focus heavily upon mitigating the risk represented by the five key areas of vulnerability referenced above. A high-level approach to diminishing the risk posed by these frequent points of attack would include the following:

- **Reducing Social Engineering Attacks:** Random background checks on system users can be very effective for reducing social engineering attacks. Other methods for reducing this risk include:
  - The use of strong password policies
  - The use of two-factor authentication for payment validation
  - Signature-on-release (using either a one-time password or physical token)
  - The deployment of automated audit roles that send out notifications for any static data changes that affect payments
  - Assigning short expiration times for one-time passwords (and automatically logging-out sessions once time has expired)
  - The use of strong Anti-CSRF protocols (CSRF: Cross-Site Request Forgery, a type of attack that results in unwanted actions on a TMS.)
  - Daily reports of user logs and permissions

- **Diminishing Fraudulent User Messages:** A multi-pronged approach to reducing fraudulent messaging would include:
  - Using audit services to send emails to a defined list of recipients whenever any static information is changed within the system
  - New or changed beneficiaries must be approved

  - Use of a fraud prevention system that monitors bank notifications for unauthorized payments
  - Email notification of any transactions that remain unaccounted for after reconciliation
  - Full audit log

- **Strengthening Weak File Transfer Protocols:**
  - Harden communication between servers through the use of firewalls.
  - Secure File Transfer Protocols, preferably using key or certification encryption, should also be available.
  - Most importantly, client should incorporate "Signing of Data at Rest" control methods such as hash-based authentication which would help prevent any tampering with the files.

- **Enhancing Employee Exit Protocols:** Software applications within an organization must be able to communicate one with another. When an employee is leaving a company, for example, the HR application should be able to send a request to other relevant applications to remove signing rights, including TMS. BAM or EBAM should also be used to notify banks that the employee is no longer a signatory on foreign accounts.

Technology Can Provide a Defense

Cyber-criminals are using technology to perpetuate payment fraud on a historic scale. But technology is a two-edged sword. And technological solutions exist that can provide a defense against all forms of fraud, both old school and cyber-based.

Leading Treasury Management Solutions should be able to help provide you with additional security providing guidance and functionality around the most effective methods to establish connections and transfer data with your banks and payment partners. Additionally, your TMS should be able to provide secure end-to-end payment workflow capabilities that:

- Restrict and control access
- Enforce segregation of duties
- Reporting on exceptions

Additionally, make sure that your treasury software provider engages in "always-on" penetration testing.

Criminals are eagerly employing technology as a weapon. Treasury professionals must be equally willing to deploy technology as a defense in the perpetual battle against fraud.

ABOUT THE AUTHOR

Ace Chaloub
Chief Technology Officer, TreasuryXpress

One of the founding members of TreasuryXpress, Ace Chalhoub is the Chief Technology Officer responsible for the overall product One of the founding members of TreasuryXpress, Ace Chalhoub is the Chief Technology Officer responsible for the overall product strategy and development of the TreasuryXpress solutions. As CTO, Ace's approach to TreasuryXpress' product strategy is to be hands on with clients to research and learn about their needs and challenges, ensuring that he continues to deliver capabilities that add value.

With an extensive background in software and solution development, Ace has spent the last decade designing mission critical systems for the financial, medical, and home automation industries. Prior to TreasuryXpress, Ace held senior technical positions at Softnet Engineering and ActiveMania.

Ace is a graduate of Notre Dame University and has a master of science in software engineering.

ABOUT TREASURYXPRESS

TreasuryXpress, a global FinTech provider and leader in frictionless treasury management solutions, was created with a simple aim – to give all companies powerful, cost-effective, and easy-to-implement Treasury Management capabilities that empower them to be able to work smarter!

Our solutions centralize 10,000+ bank accounts daily and process $7BN+ in electronic payments annually – making it easy to achieve 100% bank visibility, manage end-to-end payment processing, and distribute critical reports automatically and efficiently. And, our rapid time-to-market and diverse hosting options make it easy for treasuries to do business with us.

To learn more, visit www.treasuryxpress.com or email us at hello@treasuryxpress.com.