FACTSHEET

Treasury Security: A Complete Checklist for Fighting Digital Payments Fraud

Learn more at tis.biz »

Table of Contents

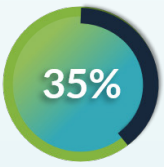
For over a decade, TIS has spearheaded a variety of industry surveys and market research initiatives. These studies, combined with extensive customer insights and industry discussions, have helped us collect millions of data points regarding the practice of treasury management and the use of treasury technology. Over time, this data and research helps us understand how new trends and technologies are impacting enterprise finance and payments operations. Ultimately, these insights enable TIS to continually improve our software suite and provide educational resources that help treasury groups navigate today's complex landscape. In this resource, we focus on treasury and payments security. We hope you enjoy this resource and find it useful.

FOUR BUILDING BLOCKS FOR TREASURY'S DIGITAL PAYMENT SECURITY

Creating a Digital Framework for Preventing & Detecting Payments Fraud

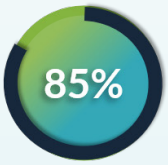
Within the past year alone, thousands of finance and treasury practitioners across the world have learned through bitter experience that digital payments fraud is rarely orchestrated by your average, everyday criminal. Rather, the vast majority of today's technology-oriented attacks, particularly those that target large enterprises, are led by sophisticated, well-funded, and innovative fraudsters. In many cases, these software-savvy perpetrators are working on behalf of state-sponsored actors or underground "black-hat" organizations. And because these groups are well-organized and well-funded, they can provide members with the latest technology and training. Ultimately, this has led to rapid digital innovation within the criminal underworld, and subsequently to a growing frequency of highly orchestrated payments fraud attacks against the corporate environment. Consisting primarily of software hacks or malware attacks, many of the most prevalent forms of fraud in existence today involve numerous layers of subterfuge and deception, which is necessary for bypassing the various security controls that organizations have in place. Common examples include the use of cleverly disguised Business Email Compromise (BEC) schemes, "Man-in-the-Middle" tactics, invoicing fraud, and the use of ransomware or other forms of "system takeover" fraud. But of course, enterprises are not entirely helpless in defending themselves. In this Factsheet, we present four building blocks that Treasury Intelligence Solutions (TIS) has designed for its cloud-based platform to support payment security. Several correlated security layers, such as regular employee training, are highlighted as well. Our hope is that practitioners can incorporate these techniques into their own security strategies and become more protected against modern-day criminals and fraud attacks. And by incorporating each of the various security layers highlighted in this guide, you can effectively prevent the vast majority of attacks from ever impacting your company. For more information about any of the highlighted security measures, use the interactive graphics at the bottom of each page.

Digital Payments Fraud in 2021: By the Numbers

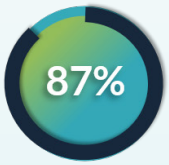


Of U.S. enterprises had a fraudulent ACH or wire pass through their security controls in the last 1-3 years.

More companies plan to increase spend on treasury security in 2021 compared to those dropping spend.



Of global enterprises believe the threat of fraud has increased or increased significantly in the past year.



Of global enterprises experienced treasury or payments fraud attempts within the past year (2020-2021).

Data by Strategic Treasurer: 2021 Treasury Fraud & Controls Survey

1 Building Block 1: The basics are vital to maintaining proper control of payments security

1. Set up basic controls through segregation of duties

The TIS platform both enables and enforces segregation of duties in the payment process across an organization. The principle of segregation of duties is based on the shared responsibility of a key process where multiple people or departments are involved. This is critical for the internal control and management of every business. The risk of error and fraud are far less manageable if a company cannot segregate duties in their payments' process.

2. Standardize payments workflows and route these through a single payments gateway

Workflow standardization across an entire organization is supported by the TIS platform. While it is not necessary to centralize your actual payments' process, it is key to bring all functions and information together using a single payments' gateway. Payments can be managed end-to-end in combination with value-added services such as validation, multi-step authorization and routing. The latter can be for different currencies, to different banks, in different countries, in different formats. Standardization of workflows and fully centralized data visibility are vital to support internal controls and audit compliance. In addition, this allows mitigation of risk in regard to payments fraud. Suspicious transactions can be tracked and monitored on one platform rather than relying on a patchwork of ERP, TMS and / or electronic banking systems etc.

3. Create a multi-layered approval process via designation of signature authority

Customers can define appropriate signature authorities for the payments' process on the TIS platform. This can mirror the current and approved business and risk processes already in place or follow a new design. A workflow may require various approvers designated by the client for payments' security or for master data safeguarding. The TIS platform currently allows for up to 10 approvers per individual payment if desired. This limit can be expanded according to a customer's needs. The above supports the flexibility to configure processes while keeping a balance between safety measures and the associated risks.

4. Regular and intensive employee security training

Although the technology components of security highlighted in this report are critical for preventing and detecting payments fraud, they only work as long as the personnel that leverage them are aware of what to look for and how to use them. For instance, if an employee neglects to install multifactor authentication to their account or forgets to delete an old employee's credentials from the payment system after they resign, the company can be exposed to significant risk. And if multiple employees are negligent in following the company's security policies, the threat of an actual loss is quite real. For this reason, corporates must develop an intentional strategy to routinely educate their employees about fraud and cybercrime, especially those that have access and /or authority over payment systems and data platforms. This education should cover information about the latest threats from fraudulent actors, as well as best practices for utilizing the security systems the corporate has in place to prevent and detect attacks.

LEARN MORE ABOUT BLOCK 1 SECURITY TOOLS

1 SEGREGATION OF DUTIES
2 SINGLE PAYMENT GATEWAYS
3 SIGNATURE AUTHORITY
4 TREASURY USER TRAINING

2 Building Block 2: Transparency and visibility are the enemies of fraud

1. Maintain real-time monitoring of all transactions and bank account activities

TIS offers clients a SaaS-based product that connects to all their banks and manages the entirety of their outbound enterprise payments. As a result, global transaction and bank account activity can be managed through a single set of interfaces in virtually real-time, with drill-down capabilities into specific regions, banks, currencies, and transactions as-needed. This drastically reduces the risk of fraud because corporate users can view and control payment activity quickly and efficiently through a single dashboard.

2. Enable regular status checks on all bank accounts using the Inventory Process

To ensure accurate and up-to-date bank account data, the TIS platform features an automated tool called the Inventory Process. Customers can use this feature on an ad hoc basis or set up regular (repetitive) status checks. Clients have the flexibility to choose which users and / or roles should be part of any review. The Inventory Process is a powerful tool for the verification of an organization's financial data. Perhaps even more importantly, it helps companies to realize their need for regular "check-ups" to detect flaws in their workflow configurations. Regular checks help identify potential fraud risks or even violations that have already occurred. For example, this tool can uncover "super users" who have been given the authority to create and approve the same payment.

3. Generate end-to-end transaction records with detailed Business Audit Logs

Audit logs encompass a chronological and immutable record of all daily activities providing full visibility into the actions of a company's staff. Complete transparency and control are maintained through detailed audit trails including changes in bank accounts and workflow configurations. Unauthorized and fraudulent activity, security violations, and possible systems flaws can be detected more quickly.

4. Leverage community data to fight fraud via Payee Community Screening (PCS)

Developed in direct response to a noted increase in invoice and BEC fraud, TIS' PCS network works by aggregating payments data across our trusted community of global enterprises and bank partners. As new payments are submitted by various enterprises through TIS, this module compares the underlying beneficiary and bank account information against a comprehensive record of all other transactions executed through the system, including those made by other enterprises in the network. By inspecting every outbound payment initiated by your enterprise in real-time against a global library of validated payments information, enterprises can strengthen their security controls by comparing transaction details against a much broader pool of data than what would ever be available in-house.

LEARN MORE ABOUT BLOCK 2 SECURITY TOOLS

1 REAL-TIME MONITORING

2 INVENTORY PROCESS

3 BUSINESS AUDIT LOGS

4 PAYEE COMMUNITY SCREENING (PCS)

3 Building Block 3: Advanced tools to support safety, security, and ease in the payment process

1. Integrate Single Sign On (SSO) into your existing IT password set-up

Security and ease of use are mutually inclusive when a customer chooses the TIS platform. Single sign-on (SSO) is an authentication scheme that allows a user to log on with a single ID and password to any of several related, yet independent, software systems and applications. The benefit of this scheme is that users do not have to enter a password and username into various systems multiple times creating a safer and more seamless process. Each entry represents a potential point of exposure. With TIS, SSO can accommodate the use of a customers' own trusted identity provider to access the TIS platform, thereby eliminating the need for additional passwords. The client's IT team can continue to have control over user access.

2. Add Multifactor Authentication (MFA) to the payment process

Two-factor authentication adds an additional layer of security and TIS recommends its use for all mission critical processes including payment approvals. MFA can prevent further fraudulent actions even if fraudsters have gained an initial foothold into a system and user credentials are compromised. Common examples of MFA include requiring a username and password combination in addition to a one-time SMS-enabled passcode, a biometric scan, or some other separately validated authentication technique when logging into a company's payment systems.

3. Ensure the integrity of payment data with specific file forwarding configurations

Customers can send payment files to the TIS platform that need to be forwarded to designated banks in their original format. By using designated File Forwarding configurations, the risk of data manipulation during the end-to-end payment process is virtually eliminated. This feature is particularly attractive for payments with a higher level of sensitivity or a higher risk level for manipulation.

4. Strengthen system & network access with biometric security

Biometric security uses the characteristics of a specific user's genes (such as a fingerprint or retinal scan) to confirm their identity when logging into company devices or payment systems. Biometrics are often combined with standard usernames and passwords to create a multifactor authentication protocol.

LEARN MORE ABOUT BLOCK 3 SECURITY TOOLS

1 SINGLE SIGN-ON (SSO)

2 MULTIFACTOR AUTHENTICATION

3 FILE FORWARDING

4 BIOMETRIC SECURITY

4 Building Block 4: Payment system and user parameters

1. Authenticate legal access to the TIS domain through IP Safelisting

IP Safelisting is a standard feature available to TIS clients. It allows users to create lists of trusted IP addresses or IP ranges, from which the access to the TIS domain is permitted. With this feature, (malicious) visits from untrusted IP addresses to the TIS platform are prevented. When used in combination with Multi-Factor Authentication, security is further increased.

2. Eliminate fraudulent beneficiaries with the Beneficiary Address Book

This feature allows customers to store master data related to all their partners, including payment beneficiaries. The type of information commonly captured includes names, addresses, bank and account details, relevant attachments (contracts and invoices) plus the legal entity this partner is associated with. Such information can easily be shared on the TIS platform with other parts of the company if required. Users must be fully authorized to create, update and delete data in the Beneficiary Address Book. Combined with the principle of multiple authorized approvers, no master data can be altered without a double check by at least one other person. This prevents payments being sent to a fraudulent beneficiary or data being subversively manipulated.

3. Allow payments to be made only to pre-defined safelists of Beneficiaries

This feature allows manual payments to be created using pre-approved beneficiaries only. Meaning, only those entities listed in the Beneficiary Address Book, the so-called Safelist of Beneficiaries, are permitted. Once loaded into a manual payment, the beneficiary data can no longer be changed. This prevents creating manual payments to a "malicious" bank account or fraudulent beneficiary.

4. Build and maintain your own list of "un"trusted parties with a blocklist

A Blocklist allows customers to build and maintain a list of untrusted parties (counterparties, banks or countries) on the TIS platform. Once implemented, every outgoing payment is checked against the list. This feature has a high level of flexibility. For example, a counterparty can be blocked by adding the Name only, or just the IBAN, or by a full set of available data (name, country, bank account details). If a payment is in the system for a blocked party, it will be stopped immediately and flagged. A blocked payment can be approved for release and processing. If it is not approved, it must be rejected. Using the Blocklist feature, a customer can block payments to be made to certain suppliers, vendors or even banks. This may be as a result of a company's "bad experience" or based on information regarding reputation etc. Companies can also use this feature to enable embargo checks or to block high-risk or sanctioned countries.

LEARN MORE ABOUT BLOCK 4 SECURITY TOOLS

See how TIS can Help Your Enterprise Become More Secure

When combined with other recommended digital security features like the use of VPNs and firewalls, the tools and practices outlined in this report are incredibly successful at detecting and preventing fraudulent attacks. Of course, much will depend on the ability of your staff to properly utilize the tools at their disposal, so training is also vitally important. However, once the proper solutions are installed and in use across the company, you will be able to monitor all of your payment systems' users, transactions, and data transmission globally. You'll also be able to identify fraudulent threats in real-time, flag and review suspicious payments at the touch of a button, and quickly analyze any bank account or beneficiary detail listed in an outbound transaction. Ultimately, this multifaceted approach to security makes it exponentially harder for cyber criminals to infiltrate and target your firm because they have to bypass multiple layers of defenses. For more information about how TIS can help you manage treasury and payments security, visit our website at www.tis.biz/en.

About TIS

TIS is reimagining the world of enterprise payments through a cloud-based platform uniquely designed to help global organizations optimize outbound payments. Corporations, banks and business vendors leverage TIS to transform how they connect global accounts, collaborate on payment processes, execute outbound payments, analyze cash flow and compliance data, and improve critical outbound payment functions. The TIS corporate payments technology platform helps businesses improve operational efficiency, lower risk, manage liquidity, gain strategic advantage – and ultimately achieve enterprise payment optimization.

Enterprise payments reimagined.

Learn more at tis.biz »

TIS

Germany (+49 6227 69824-0) | United States (+1 617 955 3223)
info@tis.biz