tis

FACTSHEET

Payee Community Screening (PCS)

Fraud Prevention Through the Power of Technology & Community

TIS helps corporates prevent payment fraud through a ground-breaking solution that leverages the power of community for participating customers and partners (i.e. data and experience). This Payee Community Screening (PCS) solution enables corporates to validate beneficiary account details and better identify potential fraud before the payment instruction is sent to the designated bank.

PROBLEM

Cybercrime continues to rise, and supplier payment processes are an attractive target for fraudsters. Criminals all around the world directly target the users of ERP systems ('social engineering') to change internal master data such as beneficiary bank account details. As a result, corporates that pay thousands of supplier invoices each month cannot be fully sure that the account information stored in their ERP systems really is the supplier's authentic bank account. Automated verification of these details is also difficult to establish and typically requires significant manual upkeep. Therefore, as your organization grows in revenue and across different geographies, your exposure to fraud increases exponentially.

SOLUTION

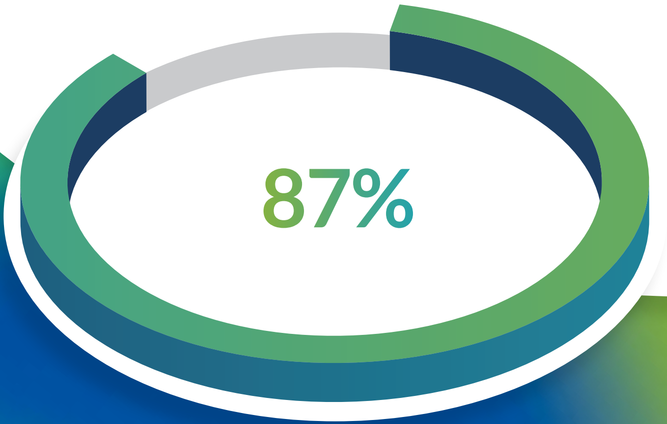
Banks conduct transaction screening (compliance filtering and monitoring) and fraud prevention activities on payments passing through their systems in order to protect themselves and their clients from harm. However, this only solves part of the problem. To protect against their own risk, corporates must also invest in integrated and technology-based security solutions, especially when it comes to payment workflows.

TIS has a strong track record in protecting its customers from fraud. Our TIS Enterprise Payment Product provides digitized straight-through processing of payments, as well as dedicated fraud prevention features such as beneficiary address book management, safe-lists and block-lists, as well as integrated alert management and compliance workflows.

Payee Community Screening is our innovative new solution which aims to increase corporates' fraud prevention effectiveness. The approach leverages multi-bank and multi-company community data with the consent of the participating corporates and under strict data protection. This approach considers the historical beneficiary and payment information of each client, of all other participating corporates, as well as a global network of banking partners. This gives a far wider and deeper pool of information and experience to identify fraud. Using various data points, the community screening runs checks to ascertain whether payment information is authentic and can be verified by other members of the community either through direct account validation via participating banks, or through historical records of completed transactions within the community. The benefits include increased control and effectiveness, plus reduced operational risk, and increased protection of the firm's reputation.

TREASURY FRAUD EXPERIENCES

87% of global enterprises experienced treasury or payments fraud attempts within the past year (2020-2021).[1]



TREASURY'S SECURITY SPEND

4x More companies plan to increase spend on treasury security in 2021 compared to those dropping spend.[1]

[1] 2021 Strategic Treasurer Treasury Fraud & Controls Survey. »

INTRODUCING TIS' PAYEE COMMUNITY SCREENING (PCS)

Developed in direct response to a noted increase in invoice and BEC fraud, TIS' PCS network works by aggregating payment data across our trusted community of global enterprises and bank partners. As new payments are submitted by various clients through TIS, this module compares the underlying beneficiary (supplier) 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. Our partnership with Deutsche Bank enhances these checks by additional account validation checks with a network of global banks, leveraging the SWIFT network and blockchain technology to verify up to 2 billion accounts globally across thousands of participating institutions.

In an environment where subterfuge and deception are a criminal's main assets, these community screening techniques are essential for ensuring that fraudsters cannot bypass your controls simply by infiltrating those of a supplier or vendor within your network. They also ensure that as soon as fraudulent or suspicious payment information is identified by one enterprise, the data is shared across the community for purposes of alerting clients about subsequent payments to that account or beneficiary.

KEY BENEFITS

- Strong (self-improving, community powered) real-time fraud prevention
- Improved global security and transparency across all connected entities and business units
- Streamlined fraud prevention processes (decreased manual workload)
- Reduced false positives (community allow-list optionality)
- Sophisticated audit-proof case management
- Flexible screening configuration (e.g., needed because of business model and risk profile)
- Rapid and easy implementation (fully integrated in TIS Bank Transaction Manager, available independently from TIS payments solution)

KEY FACTS

- Community of up to 2 billion accounts based on a bank partnership network with thousands of institutions across North America, EMEA and APAC (with 90% and more coverage in certain markets)
- Works across any ERP, HR, & Treasury System
- Protection is bank-agnostic and works for payments delivered to any financial institution that TIS connects with
- Leverages the power of all members in the PCS community to identify suspicious details
- Fundamentally self-administered
- Delivered through cloud and API technology

HOW TIS' PAYEE COMMUNITY SCREENING (PCS) TOOL WORKS

1\.

INITIATE PAYMENT

Enterprises initiate payments to suppliers and vendors in the system of their choice, which pass through to TIS.

2\.

GLOBAL SCREENING

TIS compares these payment details against the PCS community repository that spans 2 billion+* accounts and thousands of institutions.

3\.

VALIDATE OR FLAG

Vendor & account details are compared with past payments to determine if other firms can validate the payments info.

4\.

EXECUTE OR REVIEW

TIS indicates whether payments are valid and can be executed, or if underlying details are suspicious and should be reviewed.

**Data based on information provided by Onyx Liink: https://www.jpmorgan.com/onyx/liink*

WHY PCS IS CRITICAL FOR FIGHTING DIGITAL PAYMENTS FRAUD

In practice, the PCS validation process highlighted above effectively protects against four fundamental threats:

1. If you are making a payment to a new beneficiary or a new supplier bank or account for the first time, an alert will be generated by the system warning you that an additional review of the information is recommended.

2. If you are making payments to a first-time supplier which is completely unknown to other members of the PCS network, then the payment is flagged and a review workflow is initiated.

3. For vendors that you are paying for the first time, if the payment details (bank and account number combination) do not match what other enterprises in the network have used to pay this supplier previously, the payment is flagged, and a review workflow is initiated.

4. If the beneficiary or bank account details provided in an invoice ever match with a known criminal, sanctioned, or otherwise fraudulent party, the payment is automatically flagged and a review workflow is initiated. In this way, by inspecting every outbound payment initiated by your enterprise in real against a global library of payments information, enterprises can strengthen their security controls by accessing a much broader pool of data and information than what is available in-house. To date, TIS manages over hundreds of thousands of payments and $2.7 trillion in volume annually, with a network of over 40 million+ distinct beneficiaries. Combined with our support for over 100,000 unique payment formats, our library of transaction data is virtually unparalleled in the market.

   And now with the addition of PCS to our solution suite, we can better protect our enterprise clients from fraud by confirming the validity of every outbound transaction they are attempting to make.

FACTS YOU SHOULD KNOW ABOUT PCS

1. **PCS leverages community data from over 2 billion* accounts** and thousands of financial institutions in order to verify the legitimacy of new payments.

2. TIS can leverage the PCS network to scan any of the **hundreds of thousands of client payments managed through our platform** annually, which account for more than $2.7 trillion in volume.

3. The PCS network provides **24/7 continuous screening of all payments** executed by participants in the community with virtually zero downtime.

4. Any "true positive" or otherwise fraudulent payments identified through the PCS network **are automatically flagged** for all other community members moving forward.

**Data based on information provided by Onyx Liink: https://www.jpmorgan.com/onyx/liink*

LEARN MORE ABOUT HOW PCS CAN HELP YOU PREVENT & DETECT FRAUD

For TIS' enterprise clients, the Payee Community Screening (PCS) capabilities outlined in this factsheet are already becoming a pivotal component of their core security structure, and we are excited to continue deploying the solution across more global enterprises in the months and years ahead. Although no single tool should ever be relied upon to defend against all forms of fraud, it is strongly recommended that enterprises making hundreds or thousands of vendor payments every day undergo a thorough evaluation of their payment controls. More specifically, treasury and AP teams should take time to analyze whether the threat of invoice or BEC fraud leaves them exposed, especially if a vendor or supplier within their network is compromised.

For enterprises that identify gaps, we invite you to learn more about how TIS can help.

tis

Cash Flow, Liquidity & Payments.

LEARN MORE AT TISPAYMENTS.COM »

TREASURY INTELLIGENCE SOLUTIONS GMBH
Germany (+49 6227 69824-0) | United States (+1 (617) 955 3223) info@tispayments.com | tispayments.com