WHITEPAPER

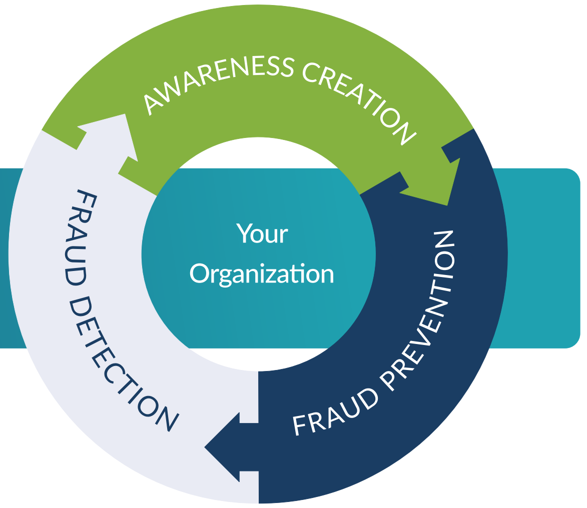
Journey Towards Better Protection Against Payments Fraud

Learn more at tis.biz »

Protecting your organization against payment fraud is a process, and it can never be done as a one-time off exercise or with one killer solution. Modern cloud and data technology have provided companies with security, but the only way to effectively fight fraud is to put proper controls in payment processes where vulnerability exists and ensure a company wide payment security strategy.

Often there is a tendency to treat fraud prevention and fraud detection as one concept but in fact they are not. In this White Paper, TIS briefly explains the difference between fraud prevention and fraud detection in corporate payments and walks you through a few major steps towards better protection against payment fraud.

Creating a positive cycle for payment security



STEP 1:

AWARENESS CREATION: SECURITY STARTS WITH PEOPLE

In its 2019 study, the Association for Financial Professionals (AFP) found that 87 percent of businesses with a revenue over one billion US dollars were subjected to fraud attempts in 2018. 43 percent of all companies in the survey lost money due to fraud.

The most common type of fraud was business email compromise (BEC). 80 percent survey respondents suffered from BEC, a yearly increase of 17 percentage points from the previous year. More than half of the companies affected lost money as a result. Fraudsters are exploiting the weakest link in every company's security system: humans.[1]

An important step to tackle fraud, therefore, is to make sure that your staff is aware of the common tactics deployed by fraudsters. This way you can increase the likelihood of suspicious activities related to fraud being spotted. Guidelines should be in place, so everyone knows how to act and who to contact. It is important that all team members receive regular trainings, as fraudsters are more innovative than you think to come up with new TTPs (Tactics, Techniques and Procedures).

For example recently, fraudsters have branched out to phone calls. Using a method called "Deepfake", a manager's voice (or in some cases an employee's or supplier's) is faked using a voice simulation software. Here, the AI recognizes patterns in intonation and convincingly recreates them. Sometimes even the correct phone number will be displayed for the fake person who calls. This is what happened at a UK-based energy firm. Fraudsters managed to get 243,000 US dollars by impersonating the chief of the German parent company, down to his accent, as the Wall Street Journal reports.[2]

It is important, however, to recognize that fraud does not always come from an external source. As the next chapter will explain, many measures to prevent fraud aim to make payment processes more transparent, so that the room for attempted fraud becomes smaller. Since measures against fraud can be restrictive or require changes in the ways of working people are used to, it is important to create awareness across the organization so that everyone is on the same page why they are necessary.

All team members must learn that they, themselves, are the weakest links in cyber security and at the same time the strongest defense against fraud for their company.

Sources:
[1] https://www.prnewswire.com/news-releases/payments-fraud-jumps-to-record-high-82-of-businesses-impacted-survey-finds-300825669.html
[2] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

STEP 2:

FRAUD PREVENTION: ENSURING AN EFFECTIVE DEFENSE

Identifying weak points

Fraud prevention starts by identifying weak points and risk factors in a company's payment processes. The following list are some of the most common examples we have seen working with different organizations. If one or more are present in your current payment processes, it is a good time to revisit your set-up and make necessary changes accordingly.

- Complex organizational structure, usually decentralized
- Lack of standardized processes, usually with multiple people involved
- No integration of ERP systems or other backend systems
- No straight-through processing for data integrity
- Multiple e-banking systems causing lack of transparency
- Different types of payment method
- End devices for doing payments not properly secured
- No consistent security strategy or execution

Using the right tools

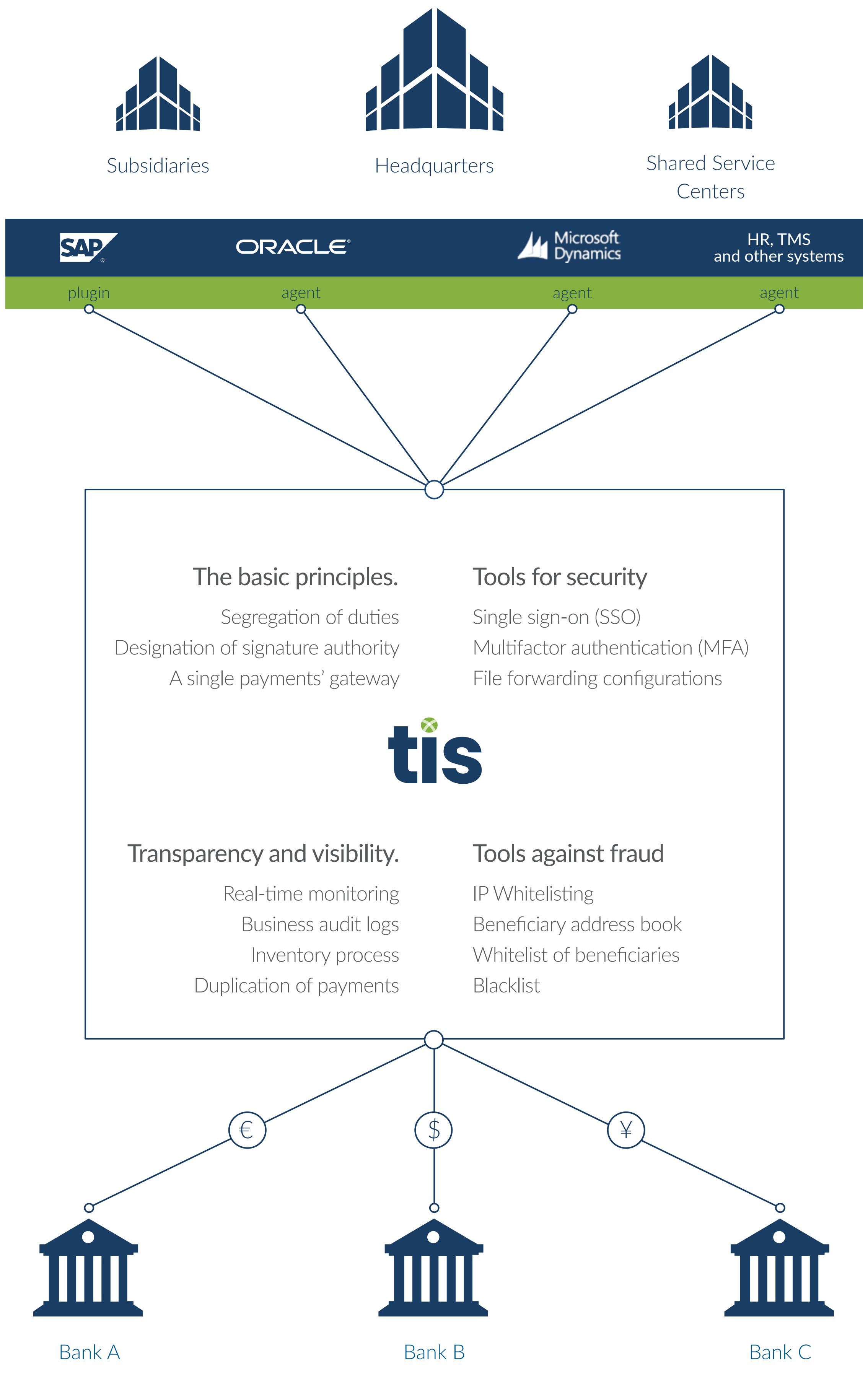
At TIS, we help many internationally renowned companies mitigate payment risks. With our cloud-based platform, all payment processes across any globally present business can be standardized and all payment data is thus centralized for visibility and accessibility. Approval processes and workflows with multiple approvers can be established quickly even across very decentralized organizations.

The picture on the next page summarizes four building blocks TIS has designed for its cloud-based platform to support payment security. With these proper controls in place, many fraud attempts can already be prevented.

For more details on the building blocks and supporting features, please visit our website and download the factsheet:

Managing Payments' and Systems' Risk to Tackle Fraud.

Develop a picture of the existing payment and banking landscape and, where possible, incorporate future plans. Review the options available and decide what is right for your business. It could be a combination of options given the nature of your business.



The basic principles.

Segregation of duties
Designation of signature authority
A single payments' gateway

Tools for security

Single sign-on (SSO)
Multifactor authentication (MFA)
File forwarding configurations

Transparency and visibility.

Real-time monitoring
Business audit logs
Inventory process
Duplication of payments

Tools against fraud

IP Whitelisting
Beneficiary address book
Whitelist of beneficiaries
Blacklist

STEP 3:

FRAUD DETECTION: SPOTTING THE UNKNOWN AND THE HIDDEN

After well-planned and solid-constructed in-frastructure with control principles are in place to ensure an effective defense against fraud, the next step is to look into fraud detection methods. One option is artificial intelligence (AI) based fraud detection solutions, main advantage of which is to spot patterns that could otherwise remain hidden to the human eyes.

AI – or more specifically machine learning – works by feeding a computer with data and telling it how it is to be interpreted. After a while, the machine learns to see patterns and establishes an algorithm. When confronted with new data, the algorithm will interpret it based on its previous experiences. The more data it has encountered, the more accurate an AI becomes. While the accuracy of AI-based algorithms has become better and better, a false positive remains possible, as AIs work with probability.

However, AI-based fraud detection has some limitations. For one, a great amount of data is needed to properly train an AI. Most compa-nies simply do not collect enough data to do that, or not all variables have been collected consistently over the years. When the data quality is poor to start with, the accuracy of the analysis based on such data source is questionable too.

What's more, such crucial data cannot be obtained from other companies, as each company's customer and supplier base show different payment behavior. A workaround is to multiply the existing data; however, this might lead to a loss of accuracy. Patterns can only be identified if they exist – if the payment behavior varies too much between non-fraud-ulent customers, then it might be hard for the AI to give you the answers you expect.

HOW ARTIFICIAL INTELLIGENCE (AI) CAN SUPPORT FRAUD DETECTION

Data input pattern recognition alarm triggering human review

The AI is given location, time of transaction, etc. for each payment and is told whether it was fraudulent.

→

The AI learns to recognize patterns that often go hand in hand with payments fraud, like an unusual time of day.

→

After sufficient training, the AI can flag suspicious transactions in new data it is given.

→

Suspicious transactions should then be reviewed to make sure there are no false positives.

FRAUD PREVENTION AND DETECTION AT A GLANCE

	Fraud prevention	(AI-based) Fraud detection
Key feature	Preventing fraud by reducing risks and monitoring attack vectors	Detecting fraud by learning and identifying uncommon behavior
Limitations	New attack vectors need to be incorporated into the software	Strong variations in payment behavior can cause difficulties
Advantages	Easier implementation, lower costs	Scope of protection is scalable
Disadvantages	Too much controlling can slow down processes	• High costs • Difficult to realize because of complex learning processes • Company internal know-how needed
Typical customer	Every company	• Companies with huge amount of payments • Decentralized companies with heterogeneous structures • Companies with reoccurring payment patterns

Payment fraud is a real challenge for CFOs and treasurers in every business. It causes not only sizable financial loss but also serious brand or reputational damage to the affected organizations. Therefore, it is no surprise that companies will often spend time and budget looking for the next generation, "data-driven toolkit" against fraud. However, we believe that payment security is a much broader topic than just payment fraud. Therefore, payment fraud prevention or detection can only be a meaningful exercise when it is an integral part of a company's overall security strategy and that is never a single or one-time off exercise but indeed a journey of continuously learning and improving.

Visit www.tis.biz/en to request a demo and learn more about how TIS can help you with fraud.

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. Visit tis.biz to reimagine your approach to payment

Enterprise payments reimagined.

Learn more at tis.biz »

TREASURY INTELLIGENCE SOLUTIONS GMBH

Altrottstraße 31 | 69190 Walldorf | Germany

T +49 6227 69824-0 | F +49 6227 69824-97 | info@tis.biz | www.tis.biz/en