EXECUTIVE BRIEFING

The Biggest Fraud Threat May Not Be Outside Your Company

Learn more at tispayments.com »

Complacency around fraud is no longer acceptable in the real-time digital age. Proactivity is required to protect the company from threats to its financial health. Finance professionals must open their eyes to the rising need for robust fraud detection and prevention practices and take action against the growing threats of external and internal fraud, before it is too late.

Fraud currently costs businesses and individuals across the world USD 5.127 tr. each year – equivalent to 6.05% of global GDP[1]. Yet many organizations continue to underestimate the risk of fraud, or only plan far-reaching action once a fraud has occurred. As such, fraud is now one of the greatest unreduced business costs and represents a significant threat to the bottom line[2].

The cost of fraud also extends beyond direct losses, potentially leading to significant reputational impacts and threats to the top line. In fact, a leading global management consulting firm, Oliver Wyman, estimates the additional reputational loss associated with fraud to be ~140% of the announced loss[3]. In turn, reputational damage can lead to customers defecting to competitors and investors shunning the company. For example, the release of a report by a whistle-blower in August 2019 describing a $38bn accounting fraud at General Electric saw the company's share price sink close to 15% of its pre-report value[4].

What's more, PwC's 2018 Global Economic Crime and Fraud Survey highlighted negative impacts on employee morale as a result of fraud, not to mention damage to business relationships, including those with regulators. Some companies may also pay the ultimate price of fraud – business collapse. An alleged fraud at UK café chain Patisserie Valerie led to the company being plunged into administration in early 2019.The collapse followed the discovery of a £94m black hole in the firm's accounts[5].

SOURCES OF FRAUD

To understand how to improve the company's defences against fraud, it is important to first recognize potential sources of fraud can be internal and/or external. For finance and treasury functions, fraud threats are most likely to occur in the area of payments – in 2018, 82% of financial professionals reported that their organizations were targeted by payment fraudsters[6].

External bad actors are often people close to the company, so-called 'frenemies'. PwC estimates that 68% of external fraud attempts are perpetrated by agents, shared service providers, vendors and customers.

It is important to remember, however, that insiders can also "allow" or indeed commit fraud. According to the 2019 AFP® Payments Fraud and Control Survey Report, 64% of attempted or actual payments fraud resulted from the actions of an individual outside the organization – meaning that as much as 36% of threats came from internal sources[7].

Common types of internal fraud include:

- False payment requests
- Forged checks and misuse of corporate cards
- Stolen credentials for payment systems
- Over-billing of customers
- Recording of false credits
- Rebates or refunds to customers
- Pay and return schemes
- Leveraging fictitious suppliers or shell companies for false billing[8].

[1] www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf
[2] www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf
[3] www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/jul/Reputational%20Risk.pdf
[4] www.theguardian.com/business/2019/aug/15/general-electric-stock-harry-markopolos-fraud-claims
[5] www.bbc.co.uk/news/business-48736447
[6] www.jpmorgan.com/commercial-banking/insights/2019-afp-payments-fraud-control-survey-report
[7] www.jpmorgan.com/commercial-banking/insights/2019-afp-payments-fraud-control-survey-report
[8] www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf

THE BIGGEST FRAUD THREAT

One of the most common – and most fundamental – mistakes when it comes to fraud controls is believing that company guidelines and trust alone are enough. Even with the most experienced of staff in place, (internal) controls are a must.

A typical loophole that helps employees to commit fraud is having too much single control over a process, such as being involved from start-to-finish in a workflow. Segregation of duties is key to deter fraud by eliminating the ability of any one individual to be so involved in a process that they are able to abuse their power. When it comes to payments, fraud can easily occur if dual control is not in place for payment transactions.

Other pitfalls which enable fraud include:

- **Decentralization.** Regional division of labour makes it easier for fraudsters. If the center does not know what is going on, and what money is supposed to be where, it is simpler to steal and conceal funds. Siloed practices also hinder visibility – so while segregation of duties is important, co-operation and communication between teams and departments is critical. Central oversite by Treasury is key.

- **Lack of standardization.** If payments are processed in different ways in different regions, and customers have different credit terms, this can leave the door open to fraud. Use of disparate technology e.g. ERP systems also causes headaches as this hampers central cash visibility. Data uploads are unlikely to happen in real-time, which also leaves fraudsters with a window of safety.

- **Lack of transparency.** Treasury often faces a lack of transparency across bank relationships and activities especially in global business operations, leading to cash and liquidity positions which are not clear. Again, this lack of clarity contributes to a convenient environment for fraudsters.

- **Manual burden.** Any process which is not automated (end-to-end) leaves room for manual intervention – which potentially opens the door to fraud. Manual checks are generally never performed in real-time, either. So, the more manual treasury is, the longer it will take for balances and transactions to be checked and reconciled, and for any fraud to be detected.

- **Misuse of technology.** While technology and automation may contribute significantly to the fight against fraud (more on this below), companies are still getting technology wrong. Some are not using technology enough, and others are placing too much emphasis (reliance) on technology. The latter may splash out on next generation fraud detection software only to find that it does not provide the desired outcomes because the company has failed to address fundamental flaws in its processes and operating model ahead of deploying the solution.

BUILDING FRAUD DEFENCES

Taking into account the above pitfalls, what might best practice fraud prevention look like in a finance department today? And how can CFOs and treasurers stay one step ahead of fraudsters tomorrow?

As alluded to, the first step to addressing fraud is creating a centralized and standardized environment which enables complete transparency, and embraces automation. Having a platform that seamlessly integrates with other systems – and offers total cash visibility is one of the most powerful weapons in the fight against fraud. In fact, it could be argued, that running a single platform - from which finance can collect all account statements from every bank account worldwide automatically and assess liquidity positions in real time - is the 'backbone' to a robust fraud prevention approach.

By using the same platform, teams located in all global locations must perform processes in the same way as the center, which significantly reduces the potential for fraud. Such a set-up enables finance functions to standardize and automate processes across the group of companies. Payment-related tasks can still be executed on local level, however they may be approved regionally or globally and can be carried out according to a single process.

To make this happen in the smoothest way possible, a central directory of every existing account as well as a payment governance process should be mandatory. Businesses need globally valid rules for their payment transactions with detailed guidelines on the following: how accounts are managed, who can open new accounts, who must give permission for this, and the documentation necessary to do so etc.

A platform which enables real-time visibility of cash also provides huge fraud-fighting benefits. Time is literally money and by monitoring treasury in real time, it is possible to detect potentially fraudulent transactions much earlier, and even stop them in many cases.

Programs providing payment outlier solutions, which flag transactions that fall outside of the typical behaviour of the organization, may also be useful in the fight against fraud. Likewise, information gained from data analytics of a company's own data or that of others in a community (platform) can help to combat fraud by tracking payment trends – if the data is clean, reliable, and up-to-date. But these kinds of tools, like specific fraud prevention technologies, are really add-ons to the fundamental architecture outlined above, rather than a replacement for it.

TECHNOLOGY TO TACKLE FRAUD: ARCHITECTURE AT A GLANCE

The ideal fraud fighting technology set-up for finance and treasury, is a single solution that is:

- Standardized
- Centralized
- Automated
- Interoperable

And enables:

- Real-time transparency over:
  - Accounts
  - Transactions
  - Statements
  - Cashflows
- Straight through processing
- Proper segregation of duties
- Signature rights management

It is also important to note that technology, if not deployed correctly, can bring more fraud risk into the finance ecosystem. The introduction of digital technology and cloud-based payments platforms, therefore, requires companies to pay extra attention to cybersecurity. Finance leaders should liaise closely with internal IT teams to make appropriate choices of technology to integrate into the payments process. Alongside the controls outlined above, staff training and education are key for fraud detection and prevention. Also vital is instilling the correct corporate culture by setting the right tone at the top around ethical behaviour. Creating an environment in which finance and treasury team members feel able to raise concerns and question orders from senior stakeholders is key.

TAKING THE LEAD

In conclusion, the biggest fraud threat for finance and treasury functions does not lie outside the organization. Rather, it is failing to implement and support the correct internal culture, controls and systems' architecture to enable fraud prevention and early detection.

CFOs and treasurers, therefore, have a growing role to play in fostering a fraud-aware mind-set. Finance leaders must take full responsibility for educating their teams, as well as their cybersecurity. The latter includes extensive vetting of solution providers to ensure that all systems are appropriate and fit for purpose. After all, as part of a holistic approach to fighting fraud, the correct technology set-up can enable companies to protect themselves against manipulation and fraud and, ultimately, loss of money and reputation.

Given extensive discussions with many clients as well as experts in the field of Fraud and Cyber Crime, here is a list of recommendations to avoid payment fraud:

- Arrange complete visibility of all bank accounts and authorized users and their rights – you can only manage what you see
- Full cash flow transparency is needed – this includes all bank accounts through an independent channel (segregation of duties)
- Create one standardized Payment Process – fragmentation will cause an open flank for error and fraud (avoid local e-banking tools)
- Manual Payments are to be avoided whenever possible – one-offs are a playground for CEO fraud – exceptions must be well defined including user limits
- Strict and verifiable audit trails that allow robust control are a must
- Avoid giving single users end-to-end responsibility – make sure that you require multi-layer approvals at the correct levels
- Taylor limits to each user or type of user / user group – this includes not only actions and functions, but also payment limits per user
- Limit the (re)input of payee data – this will reduce both human error and fraud potential – use a pre-approved address book
- Use filtering and flagging techniques – this will identify problems that might be missed through straight-through processing – such as blacklists and whitelists
- Establish payment outlier detection – this will identify problems that might be missed through straight-through processing as well

At TIS, we offer a secure, cloud-based platform which acts as a single point of contact for the entire finance function, allowing all payment transactions to be combined in a uniform way across the company. The platform also offers real-ti me cash visibility, ensuring payment procedures and cash flow are controllable at all ti mes. To find out more visit www.tis.biz and request a demo.

Learn more at tispayments.com »

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 tispayments.com »

tis

TREASURY INTELLIGENCE SOLUTIONS GMBH

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

Data contained in this document serves informational purposes only. National product specifications may vary. Printed on environmentally friendly paper. These materials are subject to change without notice. These materials are provided by Treasury Intelligence Solutions GmbH for informational purposes only, without representation or warranty of any kind, and Treasury Intelligence Solutions GmbH shall not be liable for errors or omissions with respect to the materials. The only warranties for Treasury Intelligence Solutions GmbH solutions and forth in the express warranty statements accompanying such solutions and services, if any. Nothing herein should be construed as constituting an additional warranty.