Deutsche Bank
Corporate Bank

A corporate's guide to payment fraud prevention

#PositiveImpact

flow
SPECIAL

A corporate's guide to payment fraud prevention

Payment fraud is one of the biggest challenges facing corporate treasurers today, with criminals targeting corporations of all sizes, and across all industries. Fraudsters are achieving access through increasingly sophisticated techniques, which are outlined in this guide through a series of definitions and case studies. It means that for all stakeholders within the payment industry, there is a constant battle to keep pace with new fraud methods. But, as this guide reports, corporates are not alone in this fight, and can rely on the combined abilities of their banking and technology partners for support. The whole, when fighting fraud, is greater than the sum of its parts – and a holistic approach that focuses on the strengths of each stakeholder can help provide corporates with robust defences against fraud attacks

Deutsche Bank contributors

Ole Matthiessen, Global Head of Cash Management, Deutsche Bank

Stefan Fruschki, Head of Transaction Surveillance, Deutsche Bank

Thomas Stosberg, Cash Management Structuring, Germany, Deutsche Bank

Andreas Hauser, Head of Fraud Prevention Management, Transaction Surveillance, Deutsche Bank

Ramon Schuerer, Global Head Fraud Risk Management, Deutsche Bank

Andreas Avato, Product Manager, Fraud Prevention, Channel Fraud Detection, Deutsche Bank

Published in May 2022

Contents

Foreword

Payment fraud prevention is a major challenge for corporate treasurers globally – and it is one that has yet to be comprehensively addressed by the industry. No one is safe, with criminals targeting corporations of all sizes, across all industries.

The first step in finding a solution is understanding the challenge; why is it that corporates are seemingly on the back foot when it comes to payment fraud? The answer itself is simple. While anti-fraud strategies for corporates are steadily improving, so are the strategies being employed by fraudsters to circumvent them. Fake-invoice scams, man-in-the-middle attacks and business-email-compromise are among the most common techniques used to commit fraud – and, where successful, typically lead to an average loss of US$200,000 per incident.[1]

In this sense, it is a constant game of cat and mouse. Where corporates have, for example, implemented state-of-the-art payment systems with fully integrated anti-fraud measures, fraudsters have, in turn, wasted no time in shifting their focus to other weaknesses in the chain, such as human error. To combat this, awareness training is a top priority for corporates – but here too, cyber criminals have responded by employing increasingly elaborate methods. These include social engineering and email compromise attacks which, when performed over a period of months – or even years – enable a fraudster to build up a complex and nuanced picture of a corporate's payment processes, which can then be used to enable an attack. Neither side can afford to rest on their laurels.

It is not only the techniques being used to commit and tackle fraud that are fast evolving; there are also several other variables at play. Transformations in the payment space bring their own unique challenges. For example, while the advent of instant payments will bring huge benefits for liquidity management and the overall client experience, the speed of settlement may also create challenges when it comes to preventing fraud.

So how can companies better safeguard themselves against fraudsters? Each actor in a payment chain, whether it is the corporate, bank or technology provider, brings a unique set of skills and expertise to the table – and having these ideas and approaches exist in isolation does not produce the vital synergies. Instead, a holistic offering – one that brings together our shared experiences related to fraud prevention – can help to build a much clearer picture of the risks involved and how best to combat them.

In the following pages, we will look at the fraud-related challenges being faced today, before turning to outline how the combination of efforts from corporates, banks and technology providers can help to prevent fraud.

Ole Matthiessen
Global Head of Cash Management, Deutsche Bank

1

An introduction to payment fraud

In an increasingly digitalised world, fraud prevention has emerged as a major challenge for consumers, corporates and banks. The frequency, scope and complexity of these attacks are growing each year – with the perpetrators' professionalism increasing in step. The focus of this paper will be on how businesses, their banks and technology providers are using their combined resources to defeat those who seek to defraud multinational and mid-sized corporates.

The first step is to identify the relevant definitions. Like the perpetrators themselves, a commonly accepted definition of fraud is difficult to pin down. The term can be applied to a range of scenarios, from stealing someone's identity to finding and using a stolen card for making a payment. And what one country considers to be fraud from a legal perspective, another may not. For the sake of this paper, however, we will take fraud to mean any intentional act that involves an unjust financial loss for a third party.

We should take care not to conflate fraud with the related concept of cybercrime. Cybercrime is often an enabler for fraud, as it targets – or even produces – technical weaknesses, which in turn can be exploited for fraudulent purposes.[2] For example, a cyber-criminal might use a Trojan – a virus containing malware that is made to look like a legitimate programme – to gain access to personal data. The act of using this personal data for financial gain would be an example of fraud. For the scope of this paper, we will therefore not consider cybercrime in detail but only to the extent that it enables corporate payment fraud.

2

The challenges of payment fraud for corporates

2.1 The changing face of payment fraud

Fraud is an ever-growing threat for corporates. The Association for Financial Professionals' (AFP) 2022 Payments Fraud and Control Survey found that 71% of organisations that responded had been the victim of payments fraud in 2021.[3] This figure is unsurprising given the trajectory of cybercrime more generally, with researcher Cybersecurity Ventures reporting that it expects costs to grow by 15% annually over the next five years, reaching US$10.5trn annually by 2025 – up from US$3trn in 2015.[4] But what exactly is driving this upward trend? To understand the challenges that surround payment fraud today, means first understanding the dramatic changes that continue to shape the corporate payments space.

The focus on electronic payments

In some regions, paper-based payment instructions – be they for credit transfers or cheques – remain a convenient method of payment. The core controls that banks can employ to help protect their clients from fraud in this area is to check that each signature matches the given one on the account signature card. Inevitably, conducting the necessary manual checks take up a significant amount of time and resources, while significantly impeding straight-through processing. Such controls would also lead to additional follow-up requests – for example, in instances where the signature does not closely match the one given on the account. Yet, the discrepancy can result from various legitimate reasons, such as the signatory using a different pen or work surface than usual and not necessarily because a fraudster has tried to mimic the original. Another key strategy is the manipulation of the amount involved, for example by adding an extra number or by removing the decimal point.

As a result, electronic payments have become the standard in the corporate banking space over the past decade – and paper-based payments are now increasingly rare. In Europe, for example, over 99% of all corporate payments are now electronic. If a client does decide to send a paper-based instruction, the payment is classified as high risk – as it is known that paper-based processes open the door to a much wider universe of fraud. To match the increased risk profile, these payments are handled with great care and attention – with a particular focus on security and protocol over speed and straight-through-processing (STP) rates. Reasons that clients might still send paper-based payments are increasingly rare, but could include transactions in local markets or in emergency scenarios (e.g. following a cyber-attack).

New technologies

The underlying systems that transfer electronic payment instructions have been able to leverage technological developments to further bolster their security. The upgrade of technology often includes the adoption of tools offered by Enterprise Resource Planning (ERP) and Treasury Management System (TMS) software providers. These include fraud prevention and detection services, which were identified by 64% of participants in a recent Association of Corporate Treasurers (ACT) survey as something they either already use or plan to adopt.[5]

While fraudsters can still attack a corporate's TMS or ERP system, it takes considerable time and resources – and consequently is quite rare. Rather than attack the systems themselves, fraudsters have increasingly looked to exploit the weakest parts of the chain, such as process failures or human errors, to facilitate their activities.

Organised crime

Fraud has become increasingly sophisticated, as have the fraudsters themselves. For their attacks to be successful, a fraudster's methods and associated techniques have had to become more inventive and elaborate. This in turn has given rise to a generation of more professional fraudsters

– fuelled by new concepts, such as Fraud as a Service whereby a criminal organisation will offer tools and services to others to facilitate their fraudulent activities. For example, criminals are selling confidential corporate and supplier information, such as open account receivables that have not been paid – and fraudsters are using this to engineer targeted fraud attacks.[6]

"We are not facing beginners. What we are facing is organised crime. I usually think of it like this: an employee of Deutsche Bank, or one of our clients might be working a 10-hour day and is doing a great job in their respective field. The fraudsters are doing an equally good job in their respective field. It is not a hobby for them; it is a profession. There is a small number of amateurs trying this, but in reality the ones that are having the most success seem very well organised"

Ramon Schuerer, Global Head Fraud Risk Management, Deutsche Bank

The new generation of professional fraudsters are also adept at refining their techniques and approaches depending on the client segment they are targeting:

- Multinational corporations (MNCs) will likely have robust anti-fraud measures in place, but that does not mean they are protected from attacks. Weaknesses often lie in the complexity of the organisation – and fraudsters, for example, will target the MNC's local entities, which might not follow the same stringent processes outlined at Head Office level.
- Mid-size companies usually have less robust anti-fraud measures in place, whether through the solutions they use or the technical know-how they have to hand. As a result, these organisations have their own specific vulnerabilities when it comes to payment fraud – and are more susceptible to a wider range of attacks from fraudsters.

Social engineering

Social engineering is where a fraudster will use social channels to build up a picture of the company. While this form of manipulation can be performed in person or over the phone, the growth over recent years of social media has created new vulnerabilities for corporates. The number of active social media users has skyrocketed since the millennium – reaching more than 3.6 billion people worldwide in 2020, a figure projected to increase further to almost 4.41 billion by 2025.[7] Fraudsters are leveraging information on employees – from new starters to CEOs – posted on their social media or networking channels to build up a detailed image of the company and its organisational structure, which they can then look to exploit.

Changing regulations

In September 2019, a new EU regulation – the second Payment Services Directive (PSD2) – entered into force in Europe.[8] PSD2 seeks to make payments more secure, boost innovation and help banking services adapt to new technologies.[9]

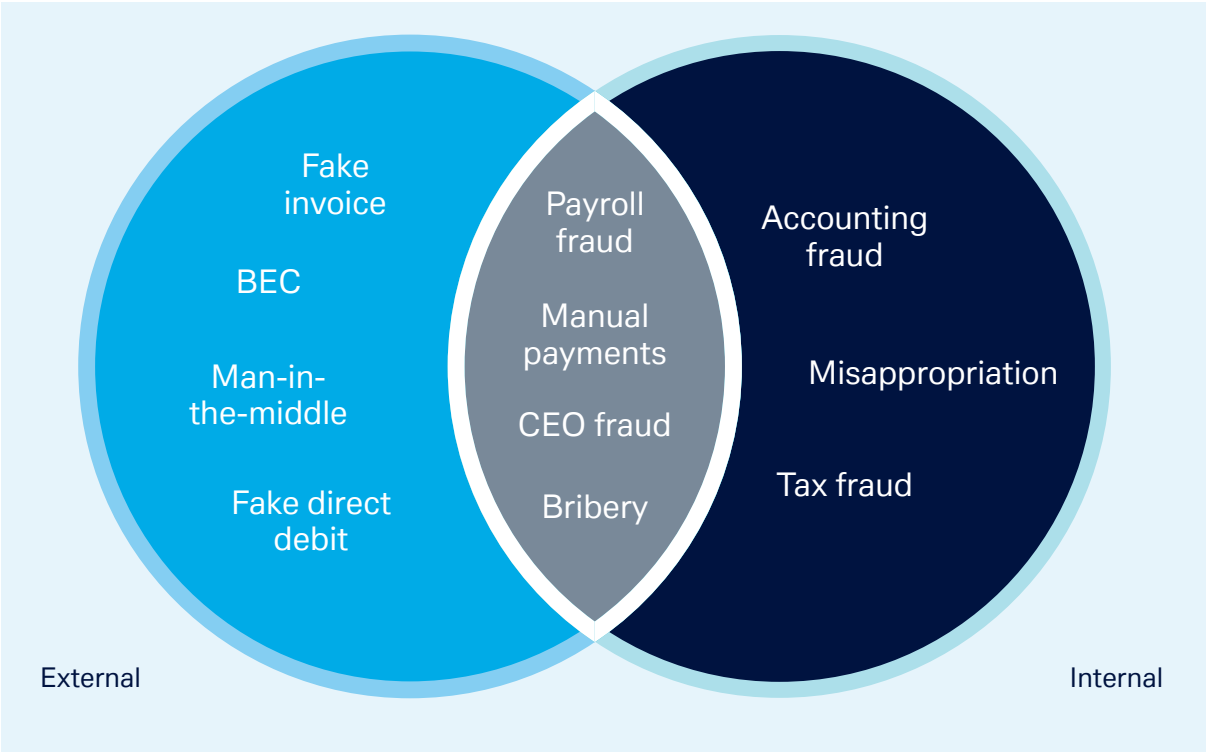
Under PSD2, as outlined in the European Banking Authority's Guidelines on security measures for operational and security risks, payment service providers (PSPs) are advised to establish and implement a 'defence-in-depth' approach to security by instituting multi-layered controls covering people, processes and technologies, with each layer serving as a safety net for preceding layers.[10] When it comes to people, this includes the implementation of the four-eyes principle (whereby every decision requires the sign off of at least two people), which, while not mandatory, is recommended. This ensures that every payment is validated by a second or even third person – allowing for any mistake to be corrected before payment execution.

When it comes to processes and technologies, one of the major developments covered by the regulation was the provision for new, stricter security requirements, known as strong customer authentication (SCA) or two-factor authentication (2FA). 2FA requires customers to provide two out of three forms of accepted authentication – something the user either knows (e.g. a one-time passcode), owns (e.g. a mobile device) or has (e.g. a fingerprint, facial recognition) – before a payment instruction can be processed. By implementing 2FA, banks have removed a section of the value chain from targeted attacks. This has made fraudsters look to alternative entry points, including communication channels and the employees at the very start of the chain.

2.2 Today's payment fraud universe

In recent years, criminals have increasingly targeted corporations across all industries, making fraud a major challenge for corporates globally. While there is no systematic, accepted overview for the types of fraud attacks – as the underlying techniques often overlap and change over time – we have grouped them into three categories for the purposes of this paper: external parties, internal parties and a combination of the two (see Figure 1). The following section seeks to outline the main techniques that corporates are facing today.

Figure 1: The corporate payment fraud universe



Source: Deutsche Bank

External vs. internal payment fraud techniques

- External fraud. The risk of unexpected financial, material or reputational loss as the result of a fraudulent action of person(s) external to the firm;
- Internal fraud. An employee of the corporation commits fraud against their employer and;
- External and internal. There are also fraud scenarios in which an external fraudster either manipulates or cooperates with an employee to commit payment fraud.

Term	Description
Accounting fraud	Accounting fraud involves the intentional manipulation of financial statements to create a false impression of a corporate's financial standing. It involves an employee, accountant, or the organisation itself misleading investors and shareholders. In the context of payment fraud, an example would be an employee expensing goods or services without properly reporting them
Bribery	Bribery is a criminal and corrupt practice where an entity offers something of value to a corporate or public official in exchange for their cooperation in influencing a decision-making process. In the context of payment fraud, this could be something as simple as a fraudster bribing an employee to give them access to the corporate's payment systems
Business email compromise (BEC)	Business email compromise (BEC) – also known as email account compromise (EAC) – is where a criminal sends an email message, which appears to come from a known source, making an apparently legitimate request. For example, a fraudster, masquerading as a vendor who the corporate regularly works with, might send an invoice with updated payment details. The corporate will change the static data as they believe the request is coming directly from the account's primary contact
CEO fraud	CEO fraud is a very specific type of attack in which a fraudster will impersonate a CEO – or other senior executive – in order to authorise a fraudulent payment (see section 2.2.1 for further insights)
Fake direct debit	Direct debit fraud can take many forms. It is often associated with identity theft, where a fraudster manages to gain access to a bank account. From here, the fraudster can pay for services and products via direct debit and use the account until its owner is alerted
Fake invoice	Fake invoice fraud occurs when a fraudster submits an invoice – or other request for payment – that is not genuine in the hope that it goes unqueried and the receiving business will pay it (see section 2.2.1 for further insights)
Man-in-the-middle (attack)	Man-in-the-middle is a type of cyberattack in which the attacker secretly relays and possibly alters the communications between two parties. The two parties continue to converse unaware that the attacker has inserted themselves in the middle (see section 2.2.1 for further insights)
Manual payments	Manual payments are no longer a part of a corporate's payment flows, but they are occasionally necessary. Typically, they are used to make one-time payments to a company or individual not in the ERP system. Such payments, however, pose a significant risk of fraud as they are challenging to track and easy to manipulate by bad actors – either internally or externally

Term	Description
Misappropriation	Misappropriation is the unauthorised use of funds for a non-intended purpose. In the context of corporate payments, this might include an employee diverting company funds into his/her own bank account
Payroll fraud	Payroll fraud is where an employee steals from a business via the payroll processing system. For example, in the context of corporate payments, the payroll staff could either create a fake employee in the payroll records or prolong the payments to an employee who has just left the company. In either case, the funds will be directed to their own account
Tax fraud	Tax fraud is where a corporate – or individual – intentionally attempt to avoid their tax obligations. In the context of corporate payments, this might include paying for goods or services in cash, without disclosing the transaction to the relevant tax authority

2.2.1 Examples of payment fraud for corporates

Based on the techniques described above, the following section sets out four typical fraud scenarios that corporates are facing.

Example 1: Fake invoice fraud

Perhaps the most common type of payment fraud is achieved using a fake invoice. A fraudster will leverage the information and format of a legitimate invoice to create a fraudulent version – changing the payee details so that when the invoice is processed, the fraudster will receive the payment in place of the supplier.

For larger amounts, corporates will likely have measures in place to ensure the supplier's invoice is authenticated before the payment is executed. However, for smaller amounts there is simply not enough time and resources to perform these additional checks, given the volume of invoices moving through the business.

Yet how does no one in the chain notice that the invoice is fake? Before making their move, fraudsters aim to gather as much information as possible on the relationship between a company and their supplier. They can then leverage this knowledge to ensure that the information, format and timing of the invoice appears legitimate – making the fake invoice very difficult to detect.

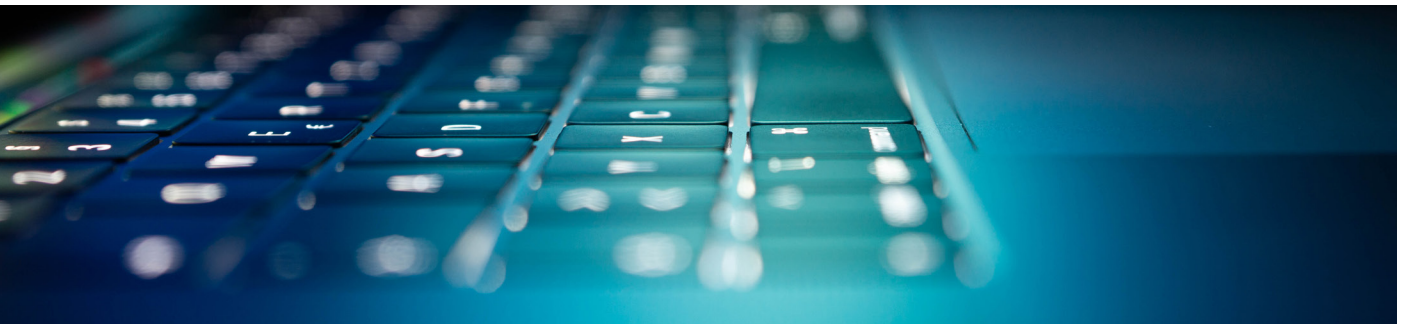
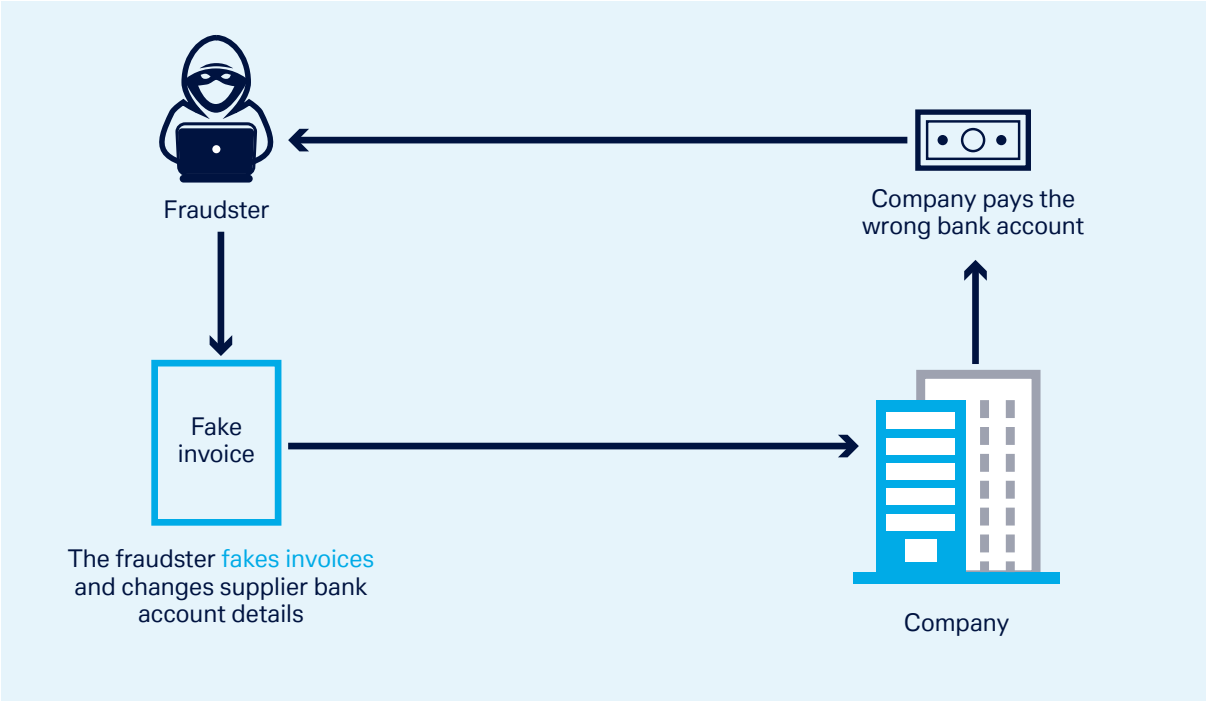


Figure 2 depicts a typical fake invoice attack. The corporate has recently undergone a publicly announced change to its organisational structure. Leveraging this information, a fraudster sends a seemingly legitimate and necessary invoice for a small amount – under the pretence that the charge relates to administrative costs. Given the circumstances, the corporate treasurer believes the invoice to be legitimate – and so goes ahead and executes the payment. This form of attack is often observed for 'one-off' services that are not covered by the buying or supplier management processes in the company's ERP systems.

Figure 2: Fake invoice fraud



Source: TIS and Deutsche Bank

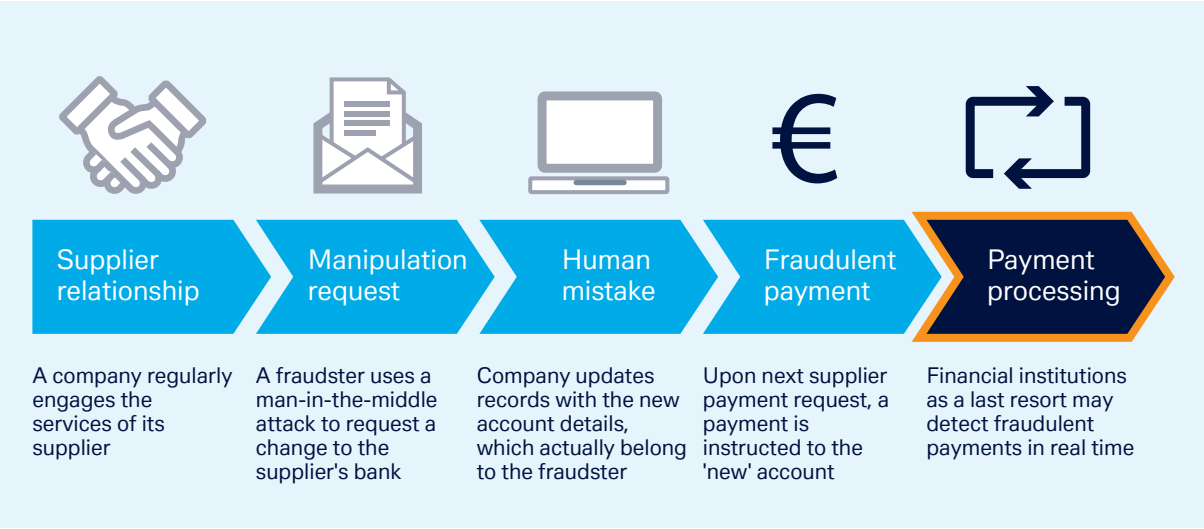
Example 2: Business email compromise (BEC) leveraging a man-in-the-middle attack

Man-in-the-middle fraud can be used to build up comprehensive knowledge of a client; for example, by hacking into the email system to read and analyse relevant mail traffic for gaining a better understanding of a company's supplier relationships.

Once the fraudster is confident of having accumulated enough knowledge on these relationships, they can initiate a business email compromise (BEC) attack from the hacked vendor to one or several of its customers. These attacks can come about either by manipulating employees to make the change (social engineering), corporate systems or a combination of both.

For example, a corporate treasurer might believe they are in touch with the supplier, when in reality an external party has placed themselves in the middle of these communications. The fraudster – using the supplier's genuine email as their vehicle – might manipulate the corporate treasurer into changing internal master data – such as beneficiary bank account details – in the ERP system. This would mean that any payments thereafter would go to the fraudulent account until alerted by either the bank, payer or payee (see Figure 3).

Figure 3: Business email compromise, leveraging a man-in-the-middle attack



Source: Deutsche Bank

Example 3: CEO fraud using more complex social engineering tactics

CEO fraud is a very specific type of attack in which a fraudster will impersonate a CEO – or other senior executive – in order to authorise a fraudulent payment. There are several avenues through which to achieve this, but most – including business email compromise, phishing, etc. – are now well known. The biggest challenge remains one of culture: are staff too scared to double check a payment if they think it comes from the top down? This aversion is being tackled through more robust procedures across the chain, as well as better education among staff.

That said, fraudsters have begun to use more complex social engineering tactics to successfully plan and execute CEO fraud. This could be achieved by leveraging the social channels of the CEO as the basis of an attack. For example, if the CEO posted that he/she was embarking on a business trip for a few days, this opportunity could be used to legitimise the attack to the receiver. Another way in which fraudsters get this information is to cold call the CEO's office in the hope that a polite receptionist might unknowingly reveal confidential information. The more information they can build up, the more likely an attack will slip through the procedural cracks.

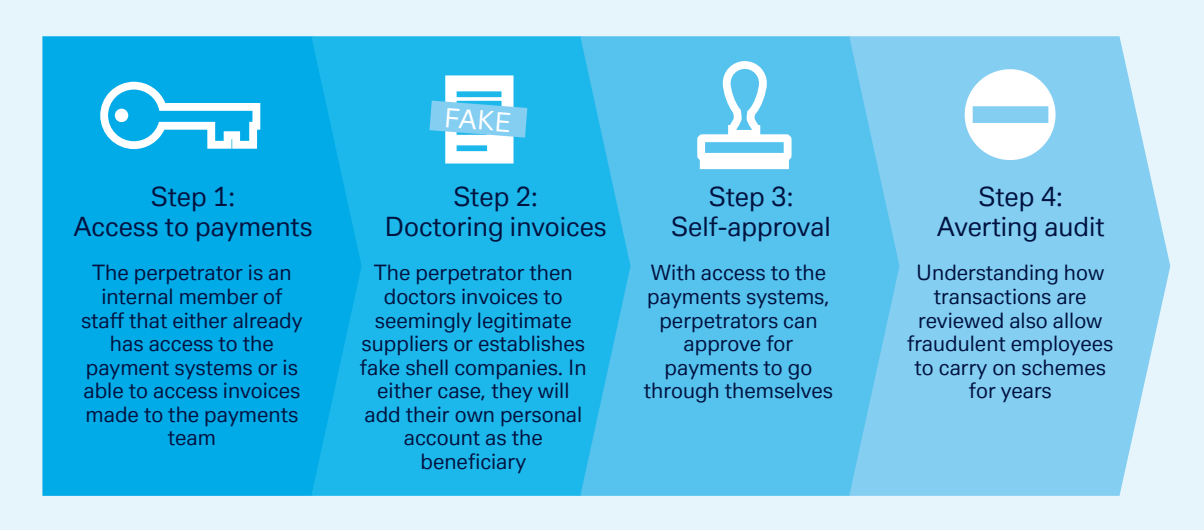
In a recent attack, a fraudster managed to find out that a foreign business partner had recently visited to meet the company's CEO. This was known by the treasury department – the target of the attack. It meant that when the fraudster contacted treasury pretending to be the CEO, the specific details of the business made the pretence appear convincing. In doing so, the fraudster was able to persuade the treasury team to execute a high-value payment on the pretext that they were acquiring the visiting company.

Example 4: Manipulation of payment processes by internal actor

Internal actors can also use their position to defraud a company. Often, a payment will need more than one signature/system approval, but this can be circumvented if the person aiming to defraud the company is conversant with the processes that are in place. For example, the individual might have worked in the department for years and established a deep level of trust with the person who is required for sign off – and, most importantly, will understand the way they work. He/she might know that this person tends to only check the size of the payment being made but not the details, such as where it is being paid.

In the example below, an internal member of staff with access to a corporate's payment systems doctors an invoice to a seemingly legitimate supplier, with their own personal account as the beneficiary. Due to either their position or another means of access – such as a colleague leaving their computer unlocked – they can approve the payment themselves.

Figure 4: Internal invoice fraud



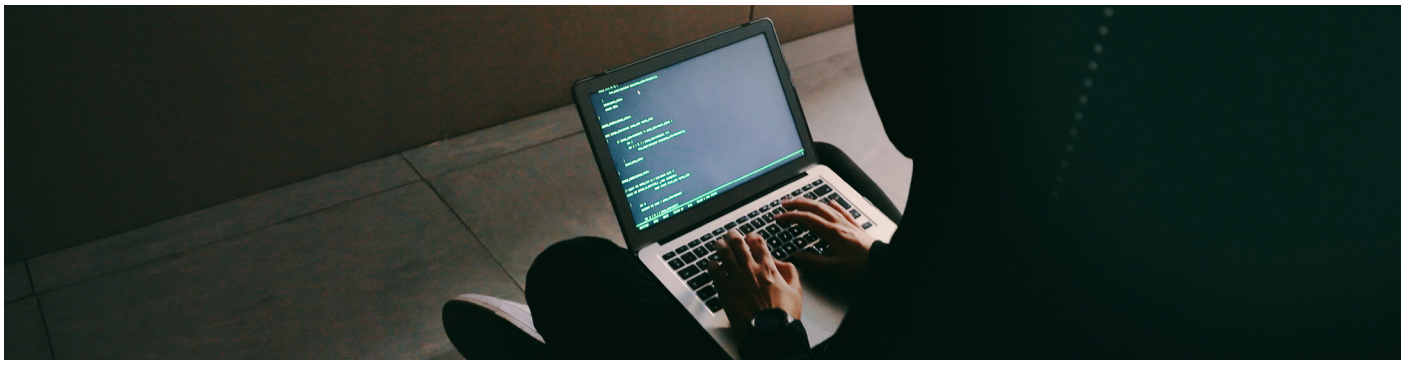
Source: Deutsche Bank

2.3 Future challenges

Instant payments

With real-time and transparent payments being increasingly used in the consumer space, a strong demand – even expectation – for similar services is emerging in the corporate space. This trend has driven the adoption of real-time payments across the globe, with over 50 countries now live with faster payment schemes.[11]

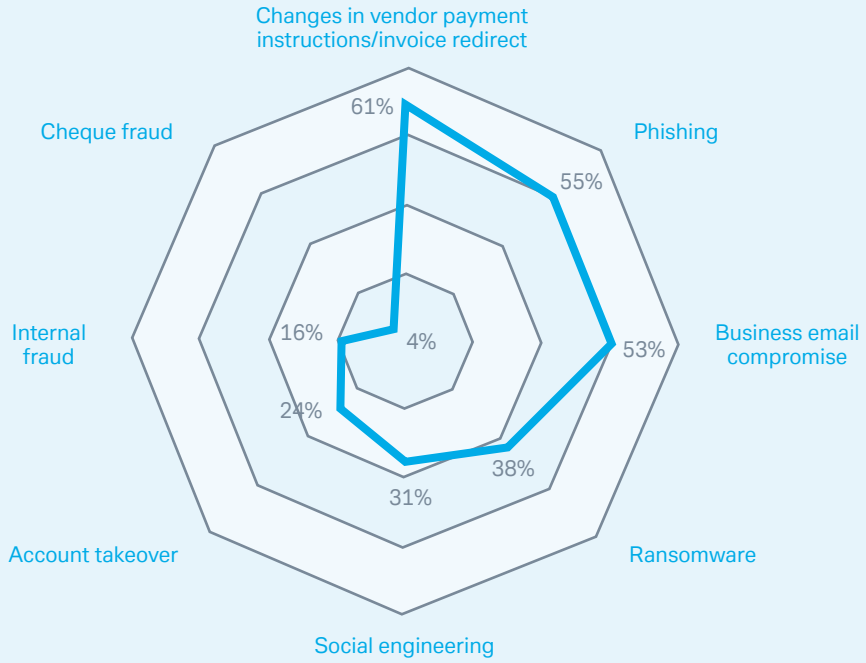
The creation of this faster payments landscape is helping to facilitate a seamless and quick end-to-end experience for corporates – and, when combined with application programming interface (API)



ACT findings on fraud

In 2021, the Association of Corporate Treasurers (ACT) and Deutsche Bank partnered on a survey designed to help treasurers benchmark their practices and operations against their peers. Incorporating responses from more than 200 corporates globally, the survey found that the most "popular" fraud scenario for the participants was "changes in vendor payment instructions" (See Example 1: Fake invoice fraud in 2.2.1 above). This scenario is often facilitated by business email compromise, social engineering and/or internal fraud.

Fraud prevention – prioritising and combating



Source: Association of Corporate Treasurers, Treasury Benchmark Survey 2021

technology, is the basis for implementing a range of real-time use cases that will play an important role in further digitalising the space. However, for all the positives, there has been an unwanted side effect: instant payments are making fraud detection harder.

Banks have a host of checkpoints, routines and processes that they use to prevent fraud. If a bank can apply this methodology across a relatively long timeframe, it has many more opportunities to ensure a payment is legitimate. With instant payments, where the necessary checks and balances often have to be performed within five seconds, banks need to be selective with the fraud prevention measures they choose to implement. So, while the adoption of instant payments will improve the client experience in the long term, it also introduces additional risks in terms of fraud.[12]

Digital assets

The digital asset universe – made up of cryptocurrencies, stablecoins and Central Bank Digital Currencies (CBDCs) – has the potential to transform the payments space. Cryptocurrencies – the most well-known of which is Bitcoin – are a form of digital currency maintained by a decentralised system using cryptography, rather than by the traditional centralised authority. Stablecoins are similar, but, unlike cryptocurrencies, their value is pegged to an asset.

- Cryptocurrency. While underlying technology boasts higher levels of security than traditional payment channels, fraudsters can find ways around them. For example, they can hack the digital wallets being used to store cryptocurrencies or set up fake wallets, which appear to belong to legitimate counterparties, and use this to request funds.[13] And as cryptocurrencies are transferred with near finality, this means that should a transaction turn out to be fraudulent it would be near-impossible to have the funds returned.
- CBDCs. The market for CBDCs is not yet mature. Among the many open questions is whether CBDCs will follow an account-based or token-based model – with the latter potentially more vulnerable to fraud. This reflects the fact that with account-based CBDCs an intermediary must verify the account holder's identity while in a token-based model the user can settle a payment without any intermediary. While this allows for higher levels of privacy, the anonymity might also bring challenges when it comes to tracing money laundering and fraudulent transactions.[14]

Machine-to-machine payments

Machine-to-machine (M2M) payments are one of the next big payment trends. M2M payments are automated, real-time payments that are made between connected devices, with minimal or no human intervention.[15] For example, this could be a machine that orders and pays for its own maintenance or a pay-per-use setup that links the technical performance of a machine (processed units, running time per day, etc.) to an automated execution of the related payment to the service provider. While M2M payments have huge potential when it comes to unlocking a digitalised process end to end, they can also open up new avenues for fraudsters – for example, hacking the machines themselves to execute fraudulent payments automatically.

3

Payment fraud prevention: A corporate perspective

While external partners can provide solutions to bolster a company's fraud-related defences, as a first step, the onus is on the corporate itself to put a robust strategy in place – one that ideally addresses four main areas: people, processes, technology and organisational structure. This chapter will describe the steps corporates can take to help combat payment fraud.

3.1 What must corporates do to avoid payment fraud?

One way in which corporates can contribute to fraud prevention of payment fraud is by using their unique knowledge to identify where risks are situated at each level of the business. A corporate's treasury function of being ahead of the curve in this area not only provides an additional layer of protection for the organisation – it adds tangible value. As a first step, corporate treasurers can apply the following framework set out in Figure 5, focussing on four potential areas of attack – of which each is vulnerable to different types of fraud attempts:

Figure 5: Corporate framework to combat fraud

Source: Deutsche Bank

3.1.1 People

Awareness is a key part of any fraud prevention strategy. All employees need to be up to date with the most popular fraud techniques, as well as their company's security protocols. Human error is one of the most common entry points for fraudsters – and awareness can help to counteract this vulnerability. Take a fake invoice scam as an example. Fraud prevention techniques, such as the four-eye principle, are preferable as the means to stop such an attack. For example, if employees know that this is a popular technique being used by fraudsters, they are more likely to ask questions – and involve more members of their team – before executing the payment. Awareness can be fostered through:

- Training. All new employees – and any member within an organisation that has not completed it already – should be provided with fraud training to ensure they can spot, and avoid falling for, the latest forms of attack being used by fraudsters.
- Regular refreshers. The world of fraud is continually evolving as hackers find new ways to commit fraud. To ensure that all members of staff are updated on the latest trends, corporates can hold 'lessons learned-sessions' in which they use near-misses logged by internal controls to train employees.
- Beware of impersonators. Email impersonators may masquerade as senior executives to direct payments staff to act unquestioningly; or as vendors to update account information. Corporates can be trained to check for red flags, such as an email containing late or sudden changes to payment instructions.
- Spot similar looking domains. Business email compromise (BEC) schemes often use similar looking email addresses that can easily be mistaken for a legitimate address. Corporates can review email address domains carefully to confirm the message is from who they think it is. When in doubt, they can confirm with known personnel from the same company.
- Verify email addresses. Perpetrators can mask email addresses by hyperlinking the real address beneath the façade of a legitimate email address. This is known spoofing, as the attacks sees the sender forge email headers so that the recipient's software displays the fraudulent sender address, which most users take at face value.

3.1.2 Processes

Corporates should review their processes and anti-fraud measures across the entire operation. That might seem no more than a common-sense step but is not without its complexities. Take a large, multinational client that operates several subsidiaries across multiple different markets. The checks and balances used by its team in Germany might be different from those used by the UK team. They may also rely on "legacy" systems that are still in use in different countries – meaning that user roles, system-supported processes and access rights vary from country to country. It is, therefore, recommended that a full audit is conducted of every process and protocol – highlighting any geographical or divisional differences, as well as ensuring that a robust framework of the respective roles and responsibilities is available and being used.

Given the nature of many fraud attacks, it is also advisable to review the IT strategy (driven from outside of the treasury function), with a focus on ensuring that the communication channels used by the corporate are as secure as possible.

Once a company has a comprehensive overview of its current practices, it can use this information to begin building a standardised fraud prevention strategy that tackles key weaknesses. The main strategies include:

- The four-eye principle. Two individuals are required to approve an action before it can be taken

- The six/eight-eye principle. For larger or more strategically important payments, three/four individuals might be needed to approve an action before it can be taken.
- The call back principle. Changes to the account are verified with the supplier via a call.
- Daily reconciliation. Perform daily or more frequent reconciliation to allow for immediate or earlier spotting of suspicious items.
- Robust escalation. Define a clear standard operating process to ensure employees can handle each issue in an efficient manner, including recording incidents and near-misses to help prevent future fraud.
- Third-party verification. Corporates can rely on bank partners or third-party vendors for trustworthy and reliable software and tools to identify and combat potential fraud.
- Pre-validation. Recently-added services are available – such as SWIFT's Beneficiary Account Validation (BAV) service, which was launched in late 2021 – that verify payee account details before an international payment instruction is sent.[16] Provided that this new service is adopted by the whole industry, SWIFT BAV has the potential to significantly reduce time spent by both banks and corporates on the management of fraudulent payments or those made with incorrect details.

Companies can also use this knowledge to better assess their risk appetite. For example, an audit of a corporate's exposures might reveal that the eight-eye principle would reduce the number of fraud attacks. However, introducing such a measure could mean implementing an entirely new payment system, which might not be cost effective when weighed against the fraud losses the company faces. In such a scenario, it could make sense for the company to focus more on education and other cheaper fraud prevention strategies instead.

3.1.3 Technology

One of the main challenges for corporates is detecting payment irregularities – such as first-time beneficiaries, urgent requests and cross-border payments (where domestic payments are the standard and vice versa) – and flagging these to the appropriate approvers. This can be achieved by an in-house fraud monitoring solution (see 3.2 Case study: How Deutsche Bahn prevents payment fraud) or one provided by an external technology vendor (see 5.2 Case study: How can technology providers help corporates prevent payment fraud?).

Whether an internal or external tool is selected, there are innovative technologies that can bolster your detection efforts. For example, artificial intelligence and machine learning is increasingly being

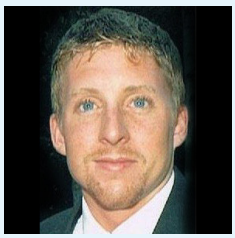
leveraged to monitor fraud patterns. These are more dynamic than traditional methods. While a rule-based model will continue to flag a payment as potentially fraudulent regardless of the human input, a machine learning-based model will learn from the human input – reducing the number of false positives, as well as fostering straight-through processing and automation.

Corporates can also use technology to improve their authentication procedures. For example, employing biometric technology – which uses physical characteristics to identify individuals as part of a multi-factor authentication policy – can provide a corporate with more robust protection as it can't be easily by-passed by stealing or hacking a device.

With so many new technologies emerging, regular technology assessments are a must in getting a feel for where existing processes might be improved, replaced or implemented, and what the different potential technology solutions could be. Implementing new tools, however, comes at a cost – so requires an evaluation of how critical it is for a company's individual risk. For a mid-cap company that has relatively regular payment flows, it might not make sense to develop a machine learning solution, whereas it could be appropriate for a multinational corporation operating across multiple jurisdictions.

3.1.4 Organisation

Understanding the structure of a large corporate is not always straightforward. It might, for example, comprise multiple branches and legal entities spread across various jurisdictions, each of which might have different departmental structures and different internal processes. Auditing and rationalising such set ups are an important first step (See 3.1.2 Processes). Once this is in place, each department – from the account payables team, finance and treasury to the account receivables team, HR and the CEO's office – involved in the transfer of funds should participate in a dedicated organisational risk assessment, with a clear segregation of duties. This can then be taken one step further and used to create a comprehensive risk matrix that incorporates every part of the business. It should be reviewed and refreshed at regular intervals.



"At Xylem, we see a range of different types of payment fraud attempts – from basic phishing emails to more sophisticated attempts, such as man-in-the middle. We have incorporated a number of steps to prevent fraud, including a standard protocol for when any bank account change request comes through via email. The first step is to call the number that is logged in our system. If a phone number is not available through the system, then we will ask for confirmation of the last two payments made, the bank account number and details of their internal contact. We then check these details against our system to confirm that it is a legitimate change. This can take from two to four weeks, which can be frustrating on the supplier side when it is a genuine request, but it is necessary."

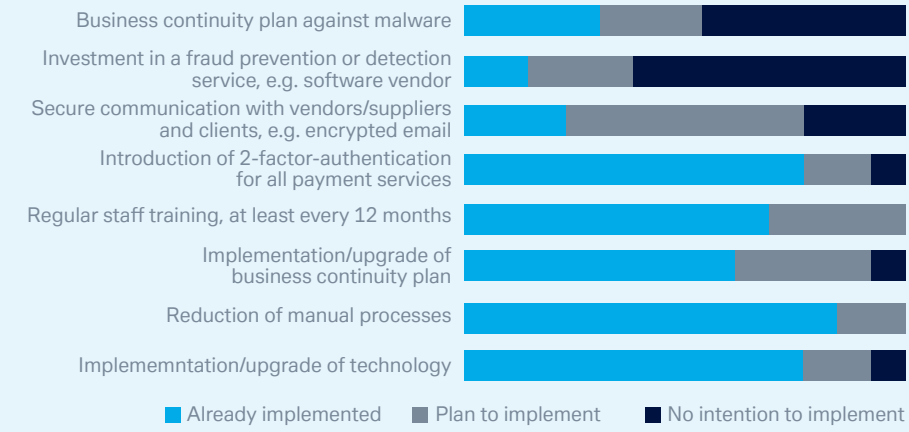
Aaron Johnston, Senior Manager, Treasury, Xylem Inc.

ACT research

As part of the ACT's benchmarking survey published in November 2021, participants were asked what methods and behaviours they have implemented– or plan to introduce – in the fight against fraud:

- 69% of participants stated they have invested in staff training, which is seen as one of the keys to avoid social engineering fraud.
- The upgrade of technology often includes the adoption of tools offered by ERP/TMS providers such as fraud prevention and detection services, which 64% of the participants already use or plan to adopt.
- The regulatory driven measures (like 2FA) have been adopted by 89% of the participants, as these created a minimum standard.
- A general key for additional protection is the (further) reduction of manual tasks and processes, agree 95% of the participants– most likely based on four-eye principle IT implementations.

Fraud prevention implementation plans



Source: ACT Benchmark Survey 2021

3.2 Case study: How Deutsche Bahn prevents payment fraud

Deutsche Bahn – the largest railway operator and infrastructure owner in Europe – was created in 1994 when Germany's two state-owned railways were combined into a single privately-run company. As of 2020, Deutsche Bahn employed 336,278 people around the globe – including 217,028 in Germany – working across 14 different business units.[17] It is, therefore, not surprising that the treasury department of Deutsche Bahn is kept busy with more than 100,000 payments each day. These can be grouped under three main categories:

- Treasury payments. These payments are low in volume, but the amounts being transferred are relatively high.
- Operational payments. These payments are high in volume, but the amounts being transferred are relatively low.
- E-commerce payments. As most of the associated fraud prevention measures lie with the payment service providers themselves (PSPs), the case study will not extend to this third category.

Treasury payments and fraud

On the treasury payments side, Deutsche Bahn leverages Treasury Intelligence Solutions (TIS) to optimise the management of its payment flows. While TIS offers fraud monitoring tools, Deutsche Bahn opted to build its own solution from scratch. Deutsche Bahn's payment data is automatically extracted from TIS and fed into the company's in-house solution through a fully integrated, resting API. The solution then analyses the contextual data of the payment instructions to determine a risk profile. The aspects being reviewed include: How often has the payee been paid? When were they last paid? How much were they paid? Based on these answers, the payments are categorised under three headings – Alarm, Warning and Information – and sent in an email to the relevant account managers:

- Alarm. For when a payment is being made for the first time. Here the respective standing settlement instructions (SSIs) are requested from the counterparty to check the data in the TIS system.
- Warning. For when a payment has been made in the past, but the previous occasion was more than three months ago. For high-value payments within this category the process described in the alarm section is followed.
- Information. For when a payment is low priority, e.g. a payment that is paid regularly

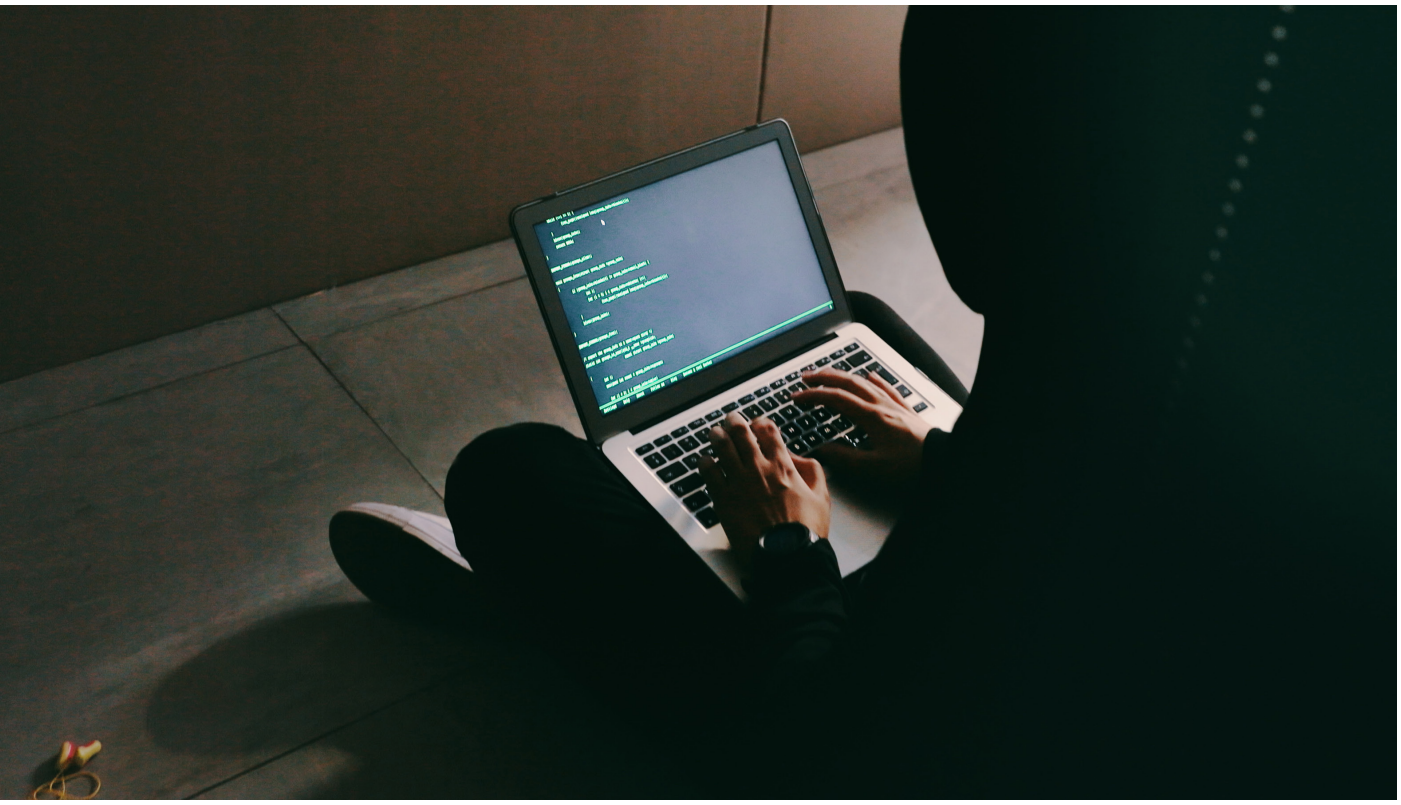
"The dangers of fraud were brought into sharp focus during the Covid-19 pandemic, which saw many of our employees, and those of our counterparties, move to a working-from-home environment. This left communication channels more exposed and, as a result, more susceptible to fraud attacks. Our in-house fraud monitoring tool, combined with our robust preventative procedures, meant that we were well placed to deal with these challenges."

Dr. Gerd Berghold, Head of Treasury Operations and Digital Treasury, Deutsche Bahn AG

Operational payments and fraud

For operational payments, successful fraud attacks are relatively uncommon for Deutsche Bahn – although they do still happen. To date, Deutsche Bahn has seen around 10 fraud cases with an overall loss in the lower five-digit euro range. Most of the attacks involve fraudulent changes to SSIs, which can be achieved using a wide array of methods, from man-in-the-middle fraud to fake invoices.

Deutsche Bahn has several procedures in place to prevent these types of fraud, including call-backs (in the case of a change to the SSI) and the four-eye process. Despite these measures being in place, human error remains a potential risk– and Deutsche Bahn has introduced regular awareness training sessions to mitigate this. Outside of the treasury function, Deutsche Bahn also ensures that it has robust IT support in place and can respond promptly in the case of a successful attack – giving the team a better chance of retrieving the stolen funds.



4

Payment fraud prevention: A bank perspective

Corporates are by no means alone in their efforts to combat fraud. They can – and should – engage with their banking partners to help better educate their employees and improve their internal processes. The following chapter will consider how banks can help corporate clients perform better in the fight against fraud.

4.1 Where do banks fit in and how can they support corporates?

Banks can support clients on three fronts: awareness creation, preventative measures and fraud detection (see Figure 6). Each of these pillars overlaps and builds on the other two – and having a strategy in place for each of them is an integral part of best practice when it comes to fraud prevention.

Figure 6: The three-step approach to tackling fraud for clients

Source: Deutsche Bank

4.1.1 Awareness creation

As noted in the previous section, the corporate itself can take several measures to prevent fraud, including by creating awareness among employees (see 3.1.1 People). This is a central part of any successful anti-fraud strategy – and one that banks can also play a crucial role in fostering.

Working closely with corporates, banks can take several measures to raise awareness of the threat

of fraud and cyber-attacks. For example, they can provide clear and precise advice on the inner workings of cash management, including information on the underlying products and services, how to safely instruct a payment, and what security measures are available for when certain end-to-end processes cannot be followed (for example, in the case of a manual or paper-based instruction). Once all parties involved have a clear understanding of what a 'normal' payment flow would look like, the focus can then turn towards improving awareness across various fraud-related topics.

Every company is different – so banks must work closely with each corporate, talking to the right people and uncovering the fine details of each individual case. These nuances often translate to significant differences. While an MNC might have centralised all its invoices to a shared service centre, the owner of a small, family-run business may still be heavily involved in the day-to-day business – including price negotiations with vendors and maintaining a strong oversight of accounts payable. The combination of flat hierarchies, fast decision making and constantly changing business models also means that start-ups present their own unique challenges. When it comes to payment fraud, these three segments come with their own unique methods of attack – requiring dedicated, tailored awareness training.

4.1.2 Preventative measures

As described above, today's fraud trends are no longer limited to classic credential theft and technical man-in-the-middle attacks on banking channels but rather focus on attacking the entire value chain leading up to the payer making a payment.

These new fraud trends are not least the result of banks introducing technical preventive measures over recent years; inducing fraudsters to seek out easier targets rather than attacking the technical bank-client communication channels themselves.

The fundamental fraud prevention controls on the banking side focus on ensuring authenticity and encryption in all bank-client communication channels be they human-to-human, human-to-system or system-to-system – to ensure that bad actors cannot easily enter the chain. Controls have been fortified in the past few years; not least due to regulatory demand and include the following key components:

- Strong (multi-factor) customer authentication (authenticity). Strong authentication is a main pillar of fraud prevention as ultimately any other control will circle around and back to verifying the identity and original intent of an authorised banking partner. Strong means of authentication is a way to verifying a digital identity, building upon a minimum of two independent authentication elements (e.g. text message and PIN). As such it is also referred to a Multi Factor Authentication.
- Secure communication (encryption). The key element besides authenticity is encryption of banking flows to prevent disclosure and manipulation of sensitive payment data by unauthorised third parties.
- Technical and operational. To augment the above measures, banks also aim to instal additional features such as automatic payment alerts or follow-up call backs in case either certain payment thresholds are breached or a change to static data is requested.

4.1.3 Fraud detection

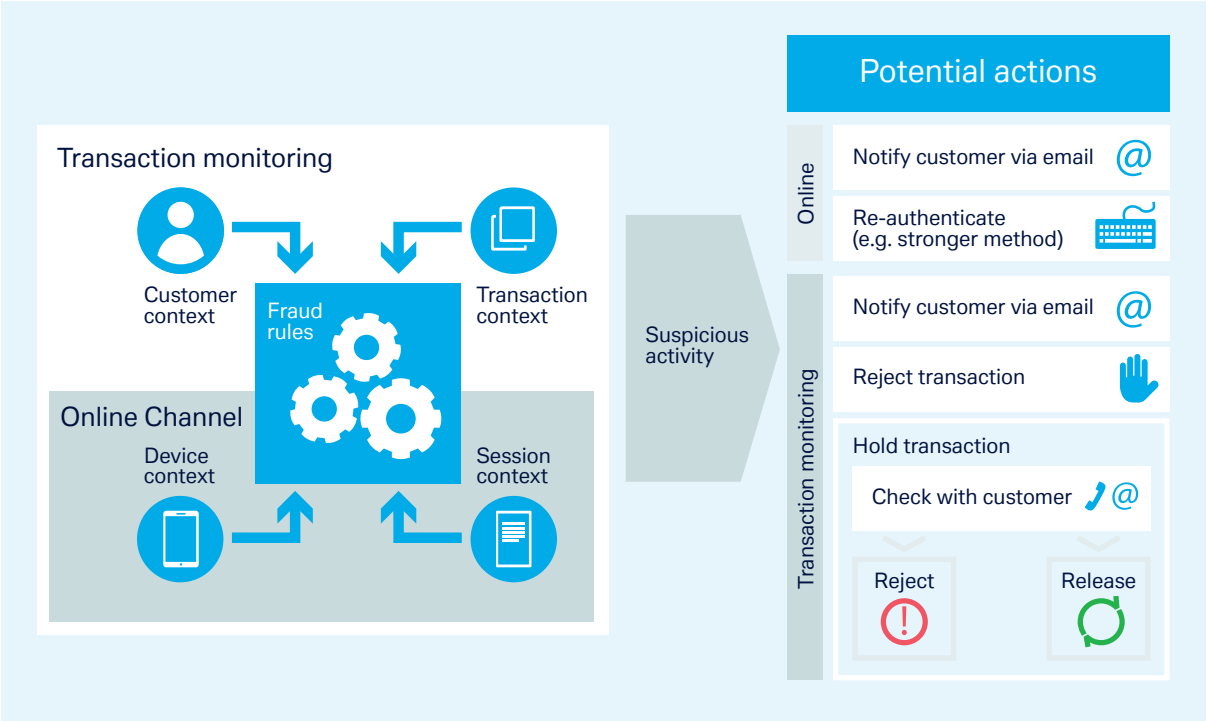
Banks will monitor both the instruction of a payment via the agreed channels as well as the transaction itself, looking at device context (the type of device used to make the payment and whether it is typical), session context (the location from which the payment was made), customer context (who the customer is, whether they have been paid before etc.) and transaction context (the type of payment, e.g. a manual payment, a payment in a batch file etc.). They then synthesise

this data to create a view as to which transactions might potentially be fraudulent (see Figure 7). Detection of known fraud schemes via rule-based surveillance include:

- Signs of bot activity. The user of an account is not human.
- Unusual device/IP. Given the user's history, the account is either being accessed through a different device or from an unusual location.
- Payment to known "money mule" account. A type of account used to transfer illegally acquired money on behalf of another actor.
- Blacklisted user/IP/geolocation. The user's IP address or the user's geolocation has previously been identified as fraudulent or risky – and blocked using a blacklist as a result.
- Parallel sessions. Two or more users are trying to access an account at the same time.
- Signs of "brute force" attack. An aspect of the account, such as the password, has undergone an attack in which all possible options are systematically entered.

Detection of these scenarios can be achieved through individual and fairly simply rules-based triggers, or via a dedicated software solution that is either built in-house or by a third-party. Once detected, several actions are open to the bank to prevent the settlement of the fraudulent transaction. For online channels this might include notifying the customer of the potentially fraudulent transaction via email or requesting additional authentication before sending the payment. On the transaction monitoring side, the bank can notify the customer via email, reject the transaction or hold the transaction while they check in with the customer (for example, a quick call with the client to confirm the transaction is indeed genuine).

Figure 7: Transaction monitoring



Source: Deutsche Bank

The problem with false positives

Today, the banking industry and its underlying corporate client customer base is still at the point where most alerts triggered by suspicious payment details are being confirmed as "false positives". At first sight, a corporate treasurer might believe that it is better to clear one more alert that turns out to be a false positive than to lose a significant amount of money because these checks were not in place. But on closer inspection, the picture is not quite as simple. Is it really worth employing two new team members to work on the alerts coming from the cash management provider? They themselves will create further effort for the company while investigating the reason for "first time use of an account of an existing vendor" and similar notifications. In this sense it fast becomes a balancing act – how much risk can a corporate treasurer take before the costs of extra resources no longer exceed the possible losses from fraud?

The mostly overlooked implication of a high rate of alerts is the human factor. Imagine a corporate treasurer on a stressful day. He/she has 100 alerts to clear before they can leave, and 99 of these are already done. The sun is out, and they want to leave the office – how diligent will they be for the final alert? Studies, as well as our own user-centric test runs, have revealed that decision fatigue plays a significant role here. Making decisions over extended periods of time can be cognitively taxing – and can lead to an unconscious preference for a "default option" that requires the least thought.[18]

4.2 Case study: How Deutsche Bank helps their clients tackle fraud

Deutsche Bank's anti-fraud framework consists of three key pillars: advisory, preventative measures and fraud detection. To take one possible scenario: a large multinational client has recently been the victim of a payment fraud attack – and is therefore seeking support on its fraud strategy from its banking partners. Further triggers for engaging in such a conversation might include a new treasurer joining, an external auditor asking for more information on the client's fraud prevention strategy or the corporate signing up for a new Deutsche Bank online channel.

But what will be discussed in these conversations and how are they being handled by Deutsche Bank? Firstly, this might include alerting customers on new cyber threats – such as information on the latest malware being used, recent cases of data losses and new types of social engineering techniques being leveraged. Such information would be packaged in a variety of ways for the client, including individual meetings, industry events, brochures and email updates – all of them regularly updated to reflect the ever-changing nature of fraud attacks. Thanks to Deutsche Bank's global network the Bank has built close relationships with local regulators, which have yielded unique insights into local fraud schemes.

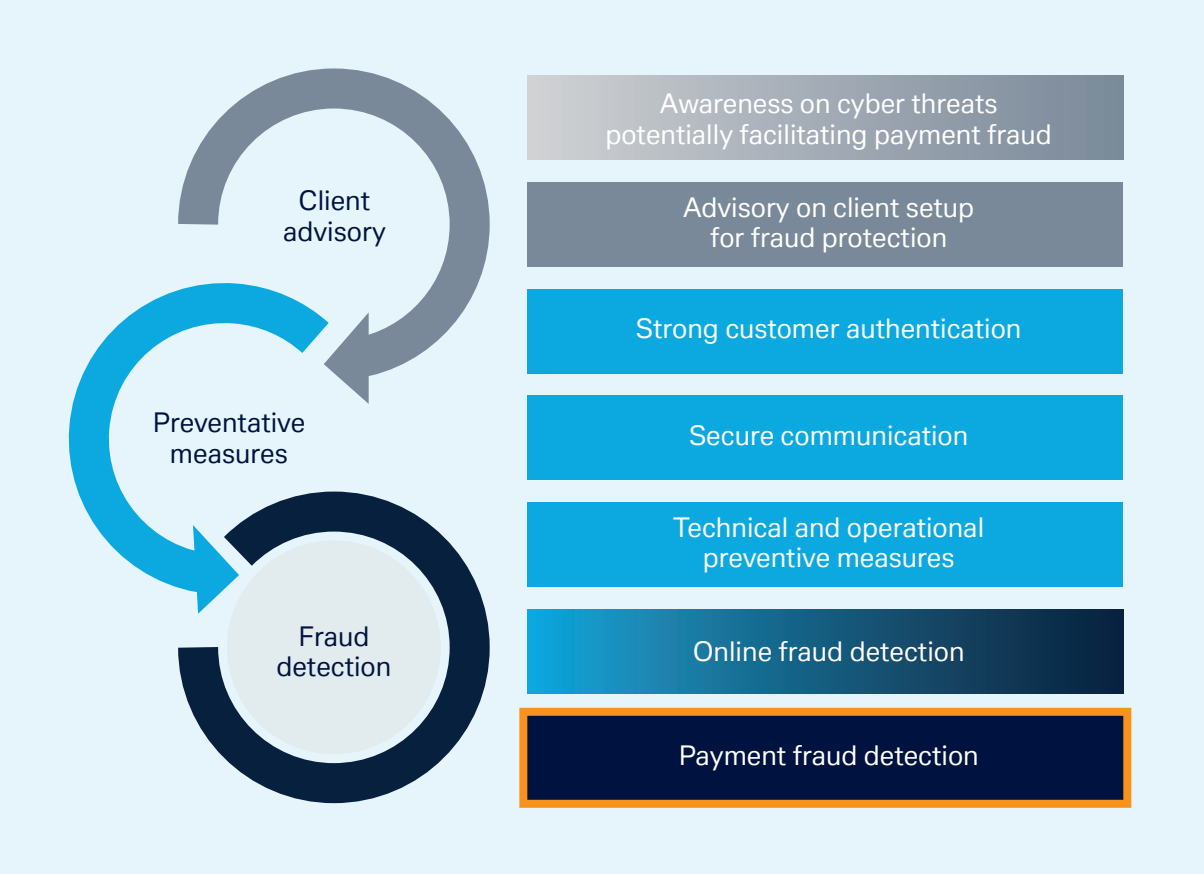
In a second step, the client might also require more information on fraud prevention. At the heart of these efforts is the Bank's day-to-day tactical dialogue, which includes over-the-phone conversations with the relationship managers in case there are any questions or payments need to be checked. In addition, Deutsche Bank also offers a host of preventative measures, including digital certificates to guarantee secure communication, and robust security measures on our online channels, such as PSD2-compliant strong customer authentication (see 4.1.2 Preventative measures).

Finally, the client may also ask about the Bank's fraud detection capabilities. Here, they can rely on several fraud detection measures Deutsche Bank has implemented:

- Online fraud detection. Alerts are provided to customers in case of an unusual event – for example, a log in from an IP address that does not fit the customer profile.
- Payment fraud detection. A scoring system rates the likelihood of a payment being fraudulent by checking against accounts related to other fraud attacks or where the payment is unusual, such as uncommon currencies, high amounts etc.

In the unlikely event that a fraud attack is successful, Deutsche Bank then works closely with the client to help them retrieve the lost funds as quickly and efficiently as possible.

Figure 8: Deutsche Bank fraud prevention and detection approach



Source: Deutsche Bank

5

Payment fraud prevention: A technology provider's perspective

A further integral part of any holistic payment fraud prevention strategy is onboarding an efficient and effective technology provider. There is now a wide array of vendors available to choose from, each offering varying levels of protection – from the foundational to the innovative. This chapter explores several key areas where technology providers are helping in the fight against fraud.

5.1 Where do technology providers fit in?

To advance fraud prevention, the technology provider market has been evolving rapidly in recent years as the industry continues to improve how it leverages data. The different fraud prevention functionalities offered by technology providers basically divide into two categories: foundational and innovative.

5.1.1 Foundational functionality

While corporates are often eager to learn about innovations in the fraud detection space, solid foundations need to be in place before implementing any innovative solutions. This is a challenge for many corporates – for instance, if a corporate works across 30 countries with 20 relationship banks, using 10 different ERP systems and with hundreds of bank accounts to pay, it can be difficult to create efficient, transparent and streamlined processes. Yet without visibility over processes, corporates are unable to even detect that fraudulent activity has occurred, never mind look to prevent it.

Therefore, having a rock-solid foundation should be a corporate's top priority – from clear audit trails and standardisation across regions, to precise governance processes and up-to-date systems. These steps will be the basis for providing transparency and visibility over payment processes.

In particular, corporates are increasingly implementing high-quality screening functionalities – such as sanctions screening – from vendors. On a more basic – but no less important – level, corporates should be able to approve and block certain suppliers (e.g. by curating a whitelist and a blacklist), agree a specific set of authorised users, implement rules for amounts over a certain threshold or in exotic currencies and have automatic alerts for when payment checks fail. These are all functionalities that corporates can implement with the help of a trusted technology vendor.

5.1.2 Innovative functionality

Many of the solutions currently available to corporates are "toolboxes" – or frameworks – that provide guidance on how a system should be configured to detect patterns and identify outliers. For some corporates, this is not enough. They want innovative, fast and compatible solutions that are ready to go – and technology providers are hard at work to deliver.

Artificial intelligence and machine learning

Payment monitoring is a major part of any fraud detection strategy and helps a corporate to spot and stop potentially fraudulent payments. This action can either be performed manually, which takes up time and resources, or via strict, rule-based systems, which can result in unwanted false positives.

New technologies, such as artificial intelligence and machine learning, are now available – and have the potential to revolutionise fraud detection. The systems using these technologies are constantly learning and adapting to a corporate's specific payment flows. This means that the system, by leveraging historic data and human actions, can reduce the number of false positives being flagged.

Swarm intelligence

One of the concepts helping to provide more innovative solutions is swarm intelligence. By joining a data pool with other businesses via the cloud, corporates can leverage community – or "swarm" – intelligence. Within this multi-tenant architecture, corporate payment data is kept securely within its own "data lake", but vendors can use the full set of data to analyse and detect fraud. For example, a supplier's bank account details can be verified using the community data. The question is simple: has someone already paid this payee in the past year? If yes, how often? If often, what was the payment behaviour? In combination, this data can help to quickly determine whether an account is legitimate – improving straight-through processing and reducing the risk of fraud.

It also means that the user can create foundational functionality – such as beneficiary screening, whitelists and blacklists and fraud alert notifications – for an entire community, based on a much broader data set. As more customers join the community, the benefits improve exponentially – raising the level enjoyed by the entire network.

Pattern matching

Pattern matching is where payment patterns are tracked and analysed – such that any atypical patterns can be flagged and investigated. Multiple contextual data items are combined and considered, with a focus on minimising the number of false positives. But how does this look in practice? Take the example of a corporate that usually pays €50,000 monthly for rent until suddenly this payment increases to €500,000. This abrupt change is worth being flagged. Or possibly a country's regulatory body decides that all fraud cases above a certain threshold – say €10,000 – must be disclosed. If a series of payments for €9,999 are being made, this pattern might indicate that a fraudster is trying to avoid detection.

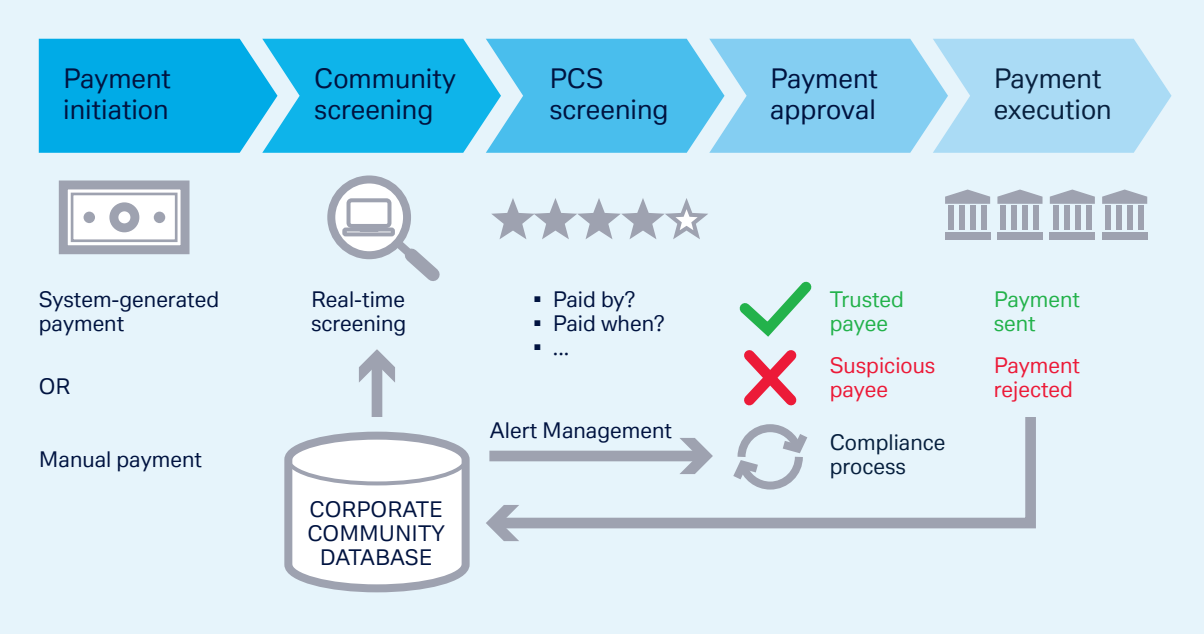
5.2 Case study: How can technology providers help corporates prevent payment fraud?

Case study: Swarm intelligence in practice

Since March 2021, TIS has partnered with Deutsche Bank to offer a Payee Community Screening (PCS) solution that leverages community data and swarm intelligence to provide fast, accurate and secure bank account verification to clients.

So how does the solution work? Once a payment in initiated in a corporate's Enterprise Resource Planning (ERP) System or Treasury Management System (TMS), it is forwarded and screened in real time by the PCS solution. The solution uses various data points to assign an overall trust score to the payment beneficiary, which is given to the organisational unit in charge of screening payments. Depending on the value of this score, an alert management system can be triggered to halt potentially suspicious payments for review. For instance, in the case of a fake invoice scenario – one of the most prevalent forms of payment fraud – the system will detect if the supplier bank account information has been changed from the number seen in the historical community data. The payment is then either approved after further checks and executed, or rejected as attempted fraud. When a fraud attempt is prevented, the company's finance team will need to be informed– as from their perspective, the supplier has been paid (see Figure 9).

Figure 9: The payee community screening solution workflow



Source: TIS and Deutsche Bank

The solution is embedded in the payment process through an API, meaning it requires no IT configuration, and works without pattern-recognition training from the corporate. As payments are screened on the customer side, the solution is also bank-agnostic – meaning that not all the corporate's banks need necessarily be involved in the scheme for it to be effective.

6

Conclusion: Fighting fraud together

As this whitepaper has highlighted, combatting payment fraud is not an issue for a single company or bank. It rather requires all stakeholders within the payment industry to work together – from the companies that fall victim to these attacks, to the banks and technology vendors looking to protect their clients and prepare for future attacks. Each stakeholder brings their own expertise to the table, ensuring that the most vulnerable areas are identified and focused on. By combining these individual core strengths, stakeholders can identify and rectify any weaknesses in their strategy – creating a holistic strategy that exceeds the sum of its parts.

Corporates

Corporates. A corporate's payment flows are complex – and can often be split across different regions, currencies, branches, subsidiaries, banking partners, accounts etc. The corporate itself will have the best visibility on the totality of these flows. In addition, it controls and understands the sources (systems and processes) as well as the triggers (e.g., month-end vendor payments) and will, therefore, have the most complete picture of its own risk-profile and corresponding appetite. Dedicated anti-fraud measures on the corporate side – developed across its people, processes, technologies and organisational structure – are an essential step in fraud prevention.

+

Banks

Banks. When it comes to corporate payments, banks provide longstanding expertise and an in-depth oversight of the entire end-to-end process. Through their extensive network, banks can gather broad insights on the various clearing schemes and local systems used across a wide variety of regions and countries. They also have a more holistic view of corporate payments, as they process payments for numerous clients of different sizes, who operate across a wide range of market segments. This gives them a unique visibility over the different types of fraud attacks that might be most attractive – and they can pass on this knowledge to their clients and technology partners to better protect the entire ecosystem from fraud attacks.

+

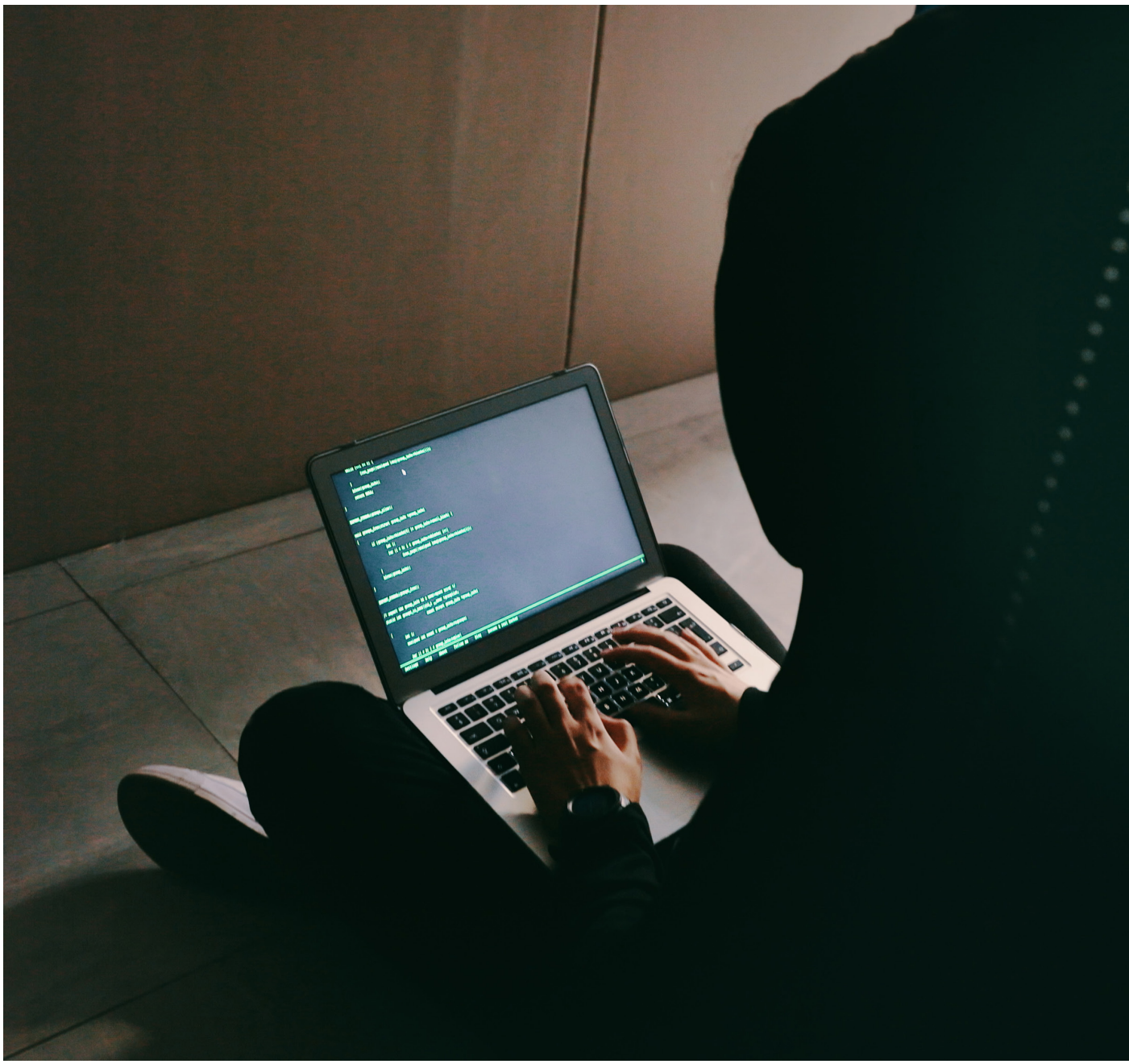
Technology providers

Technology vendors. Technology vendors and fintechs play a major role in the fight against fraud. They provide dedicated solutions that target specific areas. This is advantageous for banks and corporates alike, which can collaborate with these vendors rather than developing their own proprietary solutions. This not only saves time and resources, but also provides the entire ecosystem with better, more standardised levels of protection. Technology vendors themselves will ensure that their solutions fit to the needs and footprints of their corporate or banking clients, instead of clients having to adjust to a standardised system. This leads to optimised fraud protection where it is most effective; close to the source and close to the decision making.

=

Greater than the sum of their parts

Fighting fraud within each of these silos is ineffective. By working together, the industry can deliver greater value than the sum of its parts. And with it, corporates, banks and technology vendors can create an ecosystem that is more efficient, streamlined and, ultimately, implement strategies that work to prevent fraud – both now, and in the future.



References

[1] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

[2] https://corporates.db.com/in-focus/Focus-topics/cyber-security/

[3] https://www.afponline.org/about/learn-more/press-releases/Details/survey-percentage-of-organizations-that-report-being-victims-of-payments-fraud-activity-on-the-decline

[4] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[5] International Treasury Peer Review, conducted by The Association of Corporate Treasurers in partnership with Deutsche Bank

[6] https://chargebacks911.com/fraud-as-a-service-faas/#:~:text=Fraud%20as%20a%20Service%20is,takeover%20fraud%20or%20friendly%20fraud.

[7] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/#:~:text=Social%20media%20usage%20is%20one,almost%204.41%20billion%20in%202025.

[8] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[9] https://corporates.db.com/publications/white-papers-guides/are-you-psd2-ready-a-guide-to-the-latest-information-and-sources-of-support

[10] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[11] https://corporates.db.com/files/documents/Instant-payments-A-guide-for-corporates.pdf

[12] https://flow.db.com/cash-management/how-to-prevent-payments-fraud

[13] https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/

[14] https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-are-central-bank-digital-currencies.pdf

[15] https://www.virtusa.com/digital-themes/machine-to-machine-payments

[16] https://corporates.db.com/more/latest-news/deutsche-bank-launches-swift-s-new-beneficiary-account-verification-service-to-drive-frictionless-transactions-worldwide

[17] https://www.deutschebahn.com/en/facts_figures-6929198

[18] https://royalsocietypublishing.org/doi/full/10.1098/rsos.201059

www.db.com/flow

flow
SPECIAL