



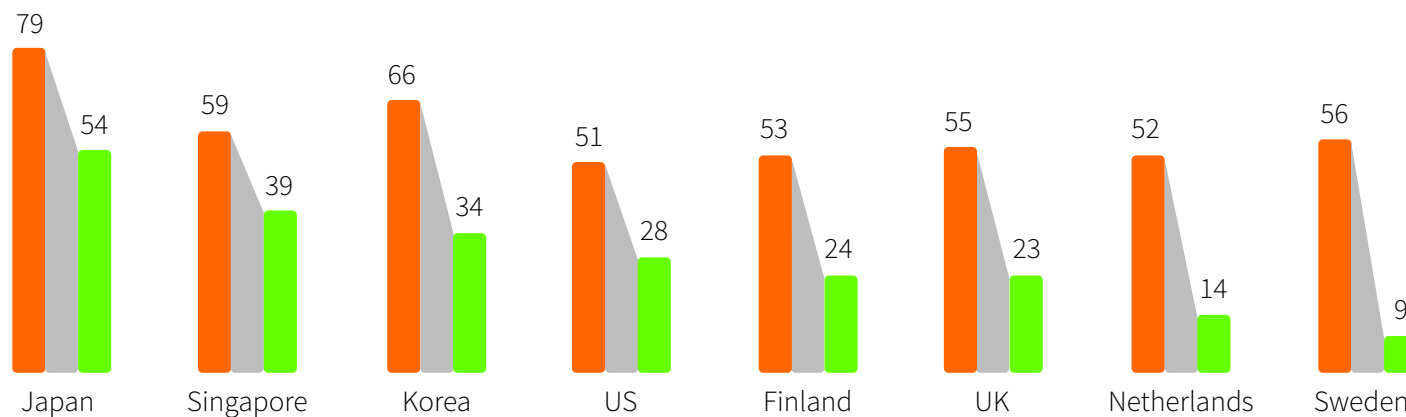
THE ANATOMY OF THE NEW FRAUDSTER

A look into the different types of fraud financial institutions need to prevent

➤ Global fraud trends

Around the world, people's shopping and payments habits have changed significantly as a consequence of the global health crisis. Lockdowns, curfews and forced physical distance have boosted e-commerce and led to a massive adoption of online payments worldwide. The pandemic has pushed cash usage to a record-low, especially in mature, digitalised countries.

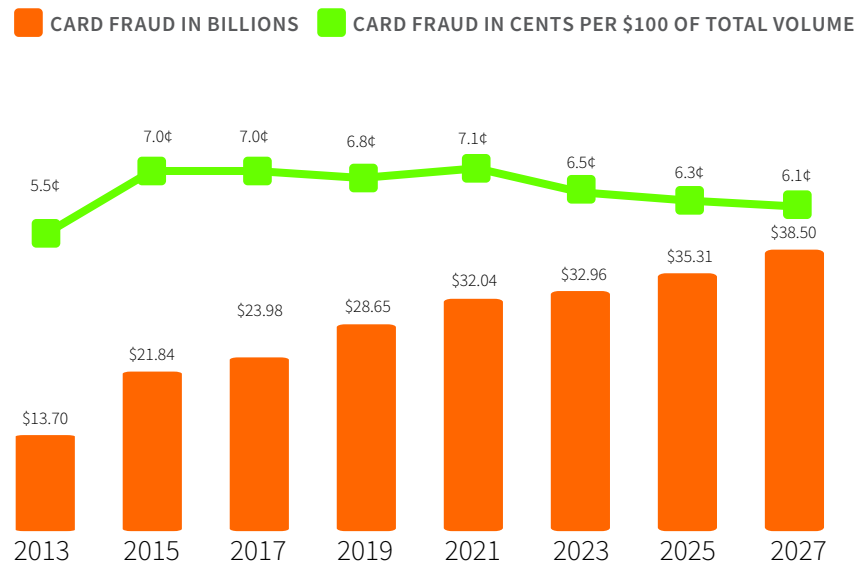
The adoption of alternative payment methods, bank apps, contactless NFC and QR codes has accelerated. Digital marketplaces such as Amazon, eBay, AliExpress, Mercado Libre, Rakuten and Zalando have seen record sign-ins. These global trends haven't gone unnoticed among fraudsters and cybercriminals. According to Lexis Nexis, the global payments market is estimated to be worth \$2 trillion by 2025, but is expected to lose up to \$200B due to fraud over the next 5 years. The payment business faces a sharp increase in card fraud, particularly in the Card-not-Present (CNP) space. CNP Fraud increased with 70% over the past few months and according to the latest Nilson report, global card fraud losses will have exceeded \$32 billion by 2021.



Mature markets • *Cashless Payment in Mature Markets (McKinsey, 2020)*

➤ Global fraud trends

In December 2020, the global Association of Certified Fraud Examiners (ACFE) published a Survey “Fraud in the Wake of COVID-19” in which 79% of the responding fraud experts said that they had seen a significant increase in fraud reports. Half of the survey respondents admitted that detecting, investigating and preventing fraud has become more difficult.



Card Fraud Worldwide • Global Card Fraud (Nilson Report 2020)

➤ CONTENT

1 FRAUD TARGETS	5
2 FRAUDSTERS' MODUS OPERANDI	8
Social engineering fraud and cross-border operations against cyber-criminals	9
Card fraud	10
Friendly fraud	11
Application fraud	12
Counterfeit fraud	12
Identity theft	13
Account take-over	16
3 WHO IS THE FRAUDSTER?	17
External fraudster	18
Internal fraudster	19
Collusion	20
4 SECURITY, DETECTION AND PREVENTION	21
Legal compliance	22
Risk management	24
Customer due diligence	25
The investigation	25
Risk assessment	26
Sanction lists	28
Card associations and regulations	28
5 CONCLUSION	29
6 USE CASES	32
DSK Bank, Bulgaria	33
TymeBank, South Africa	34
7 SMARTVISTA FRAUD MANAGEMENT SOLUTION	35

➤ 1 Fraud targets

➤ *Private companies • Banks and Telcos • Financial institutions*

With millions of people all over the world under partial or total lockdown, fraudsters shifted their modus operandi from defrauding elderly consumers to millennials. Millennials spend hours on the internet; studying, teleworking, surfing, shopping and buying products and services. This makes consumers an easy target for cyber criminals, engaged in ID Theft and other fraud schemes that will be discussed in the next chapter.

Private companies are fraudsters' preferred targets. Association of Certified Fraud Examiners - ACFE's "Global Study of Occupational Fraud" (2020) reveals that 44% of the reported fraud cases involve private companies and that these targets suffer the highest amount of financial loss.

Private companies always have been a lucrative targets for elaborate fraud schemes, especially financial institutions. Abusing "weak links" such as corruptible employees, or getting untrained personal to share private data of executives to facilitate transactions on their behalf have become popular fraud schemes which require collaboration with employees inside the company.

The pandemic forced millions of employees to work from home, which exposes companies and

government agencies to an increased cyber security risk. Home offices lack a secure infrastructure which is required to detect and prevent digital attacks on the company's network.

Banks and Telcos are attractive targets for external schemes. A global study by the Communications Fraud Control Association (CFCA) revealed that fraud cost the telecom industry over \$29B in 2018, which represented 10% of their revenue.

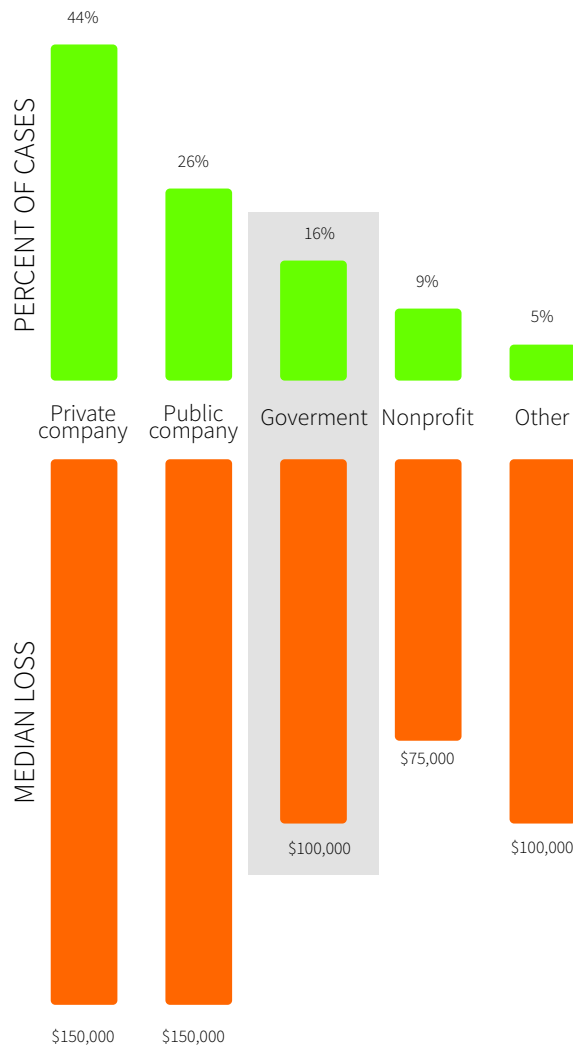
Now that consumers massively turn to mobile apps to handle their bank account(s), banks need to take extra measures to protect these apps from hackers.

Financial institutions have the financial resources to invest in Artificial Intelligence (AI) and Machine Learning (ML) powered risk-based technologies and modern identification methods such as device fingerprinting and biometrics to spot suspicious activity. These tools – which will be discussed in another chapter - enable risk departments to analyse multiple pieces of cross-channel data.

Insurance companies are forced to invest heavily in fraud expertise to manage the risk of being defrauded by false claims. This is why these companies have dedicated risk departments and fraud specialists who



➤ *The rise of e-commerce benefits fraudsters*



Global Study of Occupational Fraud • ACFE, 2020

are trained in handling high-tech case management solutions. Link analysis software is used to discover hidden connections between (false) victims and their (partnering) perpetrators in accidents, fires or when insurance companies investigate robbery, etc.

Merchants, acquirers and payment services providers (PSP) benefit tremendously from the rise of e-commerce, but so do fraudsters and cyber criminals. Like banks, all companies that manage payment transactions are of special interest to fraudsters. Being considered financial institutions, PSPs and merchant acquirers have to comply with strict rules and regulations and are obliged to apply strict due diligence processes, in order to prevent fraud, money laundering, and transaction laundering. Merchants' risk is managed by "their" payment service provider or by the acquiring banks, depending on their business models.

Fintechs have revolutionised financial services. These companies offer consumers and businesses user-friendly, digital payment methods, crowdfunding platforms and regulatory software (RegTech). Especially fintech start-ups are soft targets for criminals, because these companies tend to focus primary on product development. Young and enthusiastic innovators, who are backed by

investment companies that expect a smooth and speedy time-to-market. These fintechs have to step up their game in order to prevent financial losses and reputation damage after they launch their new product.

Governments also represent interesting targets for fraudsters. Especially, if effective control and anti-bribery measures, periodical auditing rounds, etc. are not efficiently implemented. It is fundamental to pre-screen and train all civil servants. According to the ACFE's 2020 Report to the Nations, a single case of internal fraud costs government organisations a median of \$100,000. The types of fraud that affect government organisations include public corruption, contract fraud, bribery, beneficiary frauds and false claims. In 2020, organised crime groups have defrauded the French state out of millions of euros meant for workers left jobless by the coronavirus lockdown.

Nonprofit organisations (NGO) are even more vulnerable to fraud, as they often lack anti-fraud measures, such as periodical internal audits. Interestingly, a study conducted by ACFE revealed that 51% of those who robbed NGOs were internal fraudsters; managers, supervisors or the organisation's higher executives.

➤ 2 Fraudsters' modus operandi

➤ *Fighting cyber criminals*

SOCIAL ENGINEERING FRAUD AND CROSS-BORDER OPERATIONS AGAINST CYBER CRIMINALS

Human beings are so much more vulnerable to fraud and hackers than governments or businesses. During Operation First Light, Interpol raided 33 call centers based in Asia and arrested over 1,000 people, suspected of coordinating phone scams in countries worldwide. Thousands of victims were deceived into paying money to save relatives from life-threatening diseases or disasters, or fraudsters pretended to be public officials. Assets worth \$3,47M were seized. This operation began in September 2019 and has been extended in 2021 due to the COVID-19 crisis.

Interpol, Europol and the NCB in Budapest also uncovered an international Business Email

Compromise (BEC) fraud scheme (worth \$8.6M) between a Hungarian-based company and their associates in Hong Kong, where fraudsters trick employees into transferring money to criminal bank accounts. The Interpol Orange Notice warns against the falsification, theft and illegal advertising of fake COVID-19 and flu vaccines. During the first quarter of 2020, almost 1 million COVID-related spam messages and 48,000 malicious URLs were detected. In January 2021, Europol announced that the world's largest illegal dark web market place has been taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the US and the UK. Half a million buyers and 2,400 sellers were active on this illegal marketplace. These are just a few examples of large-scale, cross-border fraud schemes.

1 million COVID related spam messages detected in the first quarter of 2020



➤ Card-not-present payment remains preferred target for fraudsters

CARD FRAUD

In countries where card penetration is high, card fraud remains the most common type of fraud. A recent 2020 graph by the US Federal Trade Commission reveals how card fraud and particularly ID theft have gone rampant. Fraudsters

use cryptocurrency to buy credit card data on the so-called darknet; data that has been stolen through phishing or hacking. Card-not-present (CNP) fraud and card-present (CP) fraud are two main types of card fraud that require different detection and prevention strategies.

- Card-not-present (CNP) payment transactions remain fraudsters' preferred target, for the simple reason that the buyer and seller do not meet in person. The anonymous nature of CNP payments makes it much more vulnerable than payment methods where cards and the buyer are physically present. CNP fraud involves the unauthorized use of specific credit or debit card numbers, security codes, expiry dates and billing addresses to purchase products and services via e-commerce websites or over the phone.

- When card data is stolen in the presence of payment cards (i.e. on ATMs, mobile POS devices) this is called card-presence (CP) Fraud. Most victims aren't aware of the unauthorised use of their cards, until they check the periodical statements. This allows fraudsters to buy time.

The wide adoption of EMV-enabled cards greatly reduced CP fraud, but it forced fraudsters to switch their modus operandi to CNP fraud schemes. The COVID-19 pandemic has accelerated the adoption of e-commerce, which boosted the rise in CNP payments; golden opportunities for fraudsters. Fraud experts say that CNP fraud has increased with 70% since the start of the pandemic.

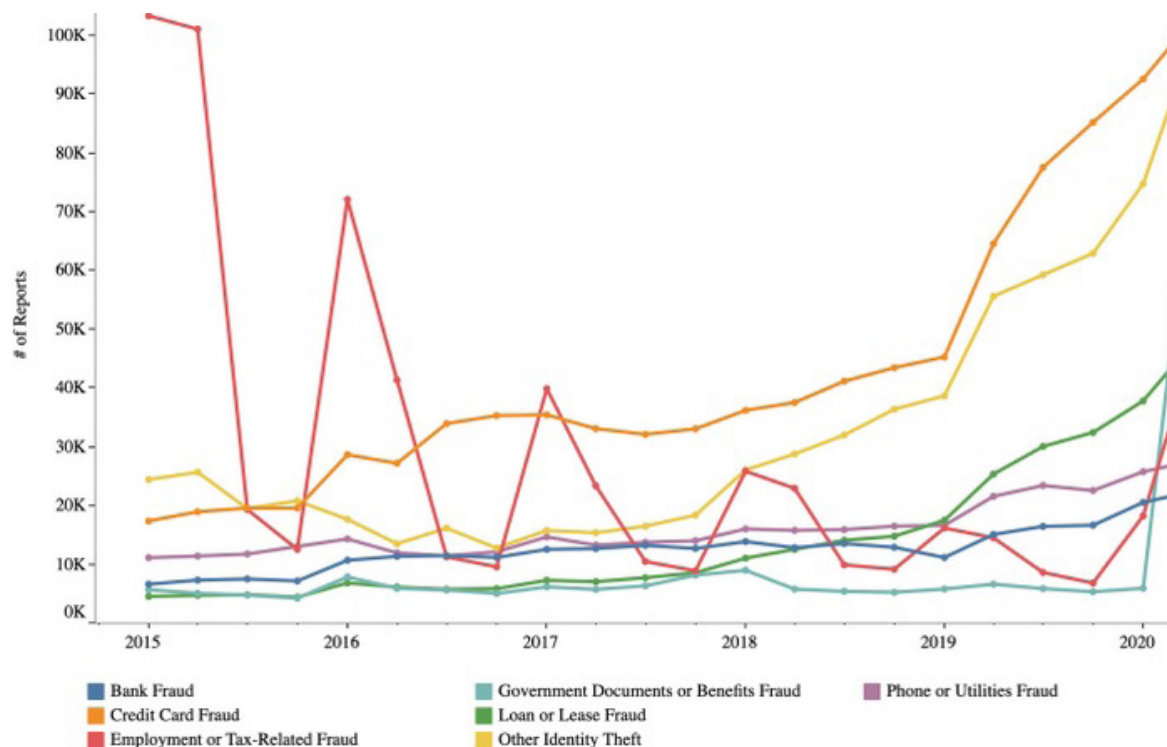
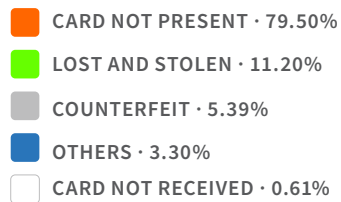


Image credit: Tableau Public • Data Source: Federal Trade Commission

➤ *Be aware of transaction laundering*



Value of fraud types as a share of total card fraud using cards issued within SEPA • *European Central Bank (2020)*

This trend is reflected in recent European fraud statistics that were issued by the European Central Bank in the ECB's yearly (2020) report. According to Juniper Research, retailers will lose an estimated \$130B in cumulative revenue due to CNP Fraud between now and 2023 and the payment industry will be spending around \$10 billion yearly on fraud detection and prevention capabilities.

Transaction laundering is another elaborate scheme to be aware of. When a merchant aggregates payment transactions on behalf of another merchant's website, without the knowledge of the merchant acquirer, this is called transaction laundering or illegal aggregation. Transaction laundering mostly involves the sales of illegal products and/or services. The merchant that acts like the mule, gets a share of the profits.

PSPs and acquirers risk reputation damage and heavy penalties imposed by the card associations. There are cases where merchants were not aware that their accounts were being abused by transaction launderers. When these merchants are confronted with hard evidence, presented by the card

associations to the acquiring bank, these victimised merchants have a really hard time to prove their innocence. This laundering scheme is under heavy scrutiny of the card organisations, because it feeds on the booming success of e-commerce.

Chargeback fraud is a time-consuming and costly affair for online merchants. A chargeback is a transaction that is disputed by the cardholder or issuing bank. The card brands offer their consumers the possibility to reclaim their transaction. When a complaint is filed, the issuing bank starts an investigation. When a merchant is being issued a chargeback, it must provide evidence that the consumer was fairly charged. If the merchant fails, he loses the sales revenue, the shipping costs, and he has to pay the chargeback fee, whether or not the cardholder's claim is rejected.

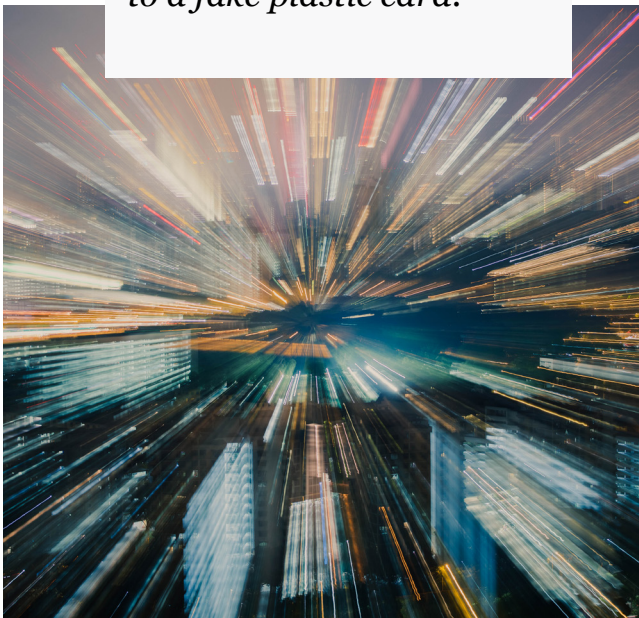
If chargebacks exceed 1% of total sales, the merchant could face a high penalty or even the termination of his account. Chargebacks are a bigger problem in the CNP environment. An estimated three quarters of all chargebacks are fraudulent and consists of friendly fraud or ID theft.

FRIENDLY FRAUD

According to the FBI, friendly fraud is one of the top

➤ Increase in social media fraud with worldwide lockdowns

Counterfeit fraud occurs when criminals skim or copy legitimate card data to a fake plastic card.



3 threats to e-commerce. It is the most common and costly chargeback fraud scheme. The majority of chargebacks consist of friendly fraud. The cardholder received the product, but lies to their bank, claiming they didn't authorise the purchase or they never received the product. The merchant loses the delivered product, the amount paid for the product and the merchant has to pay a chargeback fee for the disputed transaction.

APPLICATION FRAUD

When fraudsters apply for loans or credit cards by using their own identity, this is called first-party application fraud. After the approval, they cash the loan and disappear below the radar. 40% of application fraud involves the use of fake IDs, combining stolen data of a number of victims.

COUNTERFEIT FRAUD

Counterfeit fraud occurs when criminals skim or copy legitimate card data to a fake plastic card. Fraudsters install skimmers at gas stations, restaurants, movie theaters or ATM machines to collect card data. A hidden micro-camera may film the PIN code that is being entered. Skimming isn't easy to detect. In regions where merchants massively accepted EMV chip enabled card payments, counterfeit fraud was

reduced by 75%. (VISA, 2019).

When fraudsters 'fish' individual's private or financial data through mails, SMS or VM messages, this is called phishing, SMS'ing or vishing. A variation on this fraud scheme is the romance scam, where "romantic" fraudsters use social media and dating apps with the purpose of establishing an emotional dependency with their victim(s) and convince them to "help" the fraudster solve his/her "problems". Fraudsters could even trick their victim(s) into participating in naked video chats, which are used for blackmail/sexortion.

Reports of social media fraud scams where victims were tricked in spending huge amounts of money have tripled in 2019, with a sharp increase after the worldwide lockdowns sharply increased social media activity. The US Federal Trade Commission announced that reported losses through social media fraud scams climbed to nearly \$117M during the first half of 2020. Reported scams often related to online shopping, romance scams, and fake income opportunities. Many reports involved web shops that didn't deliver sold products and nearly one quarter of the victims were 'seduced' to buy products or services promoted through deceptive advertisements. Lost and stolen card fraud and Card-Never-Arrived Fraud occur when debit or credit cards are stolen or

➤ Identity theft targets all ages

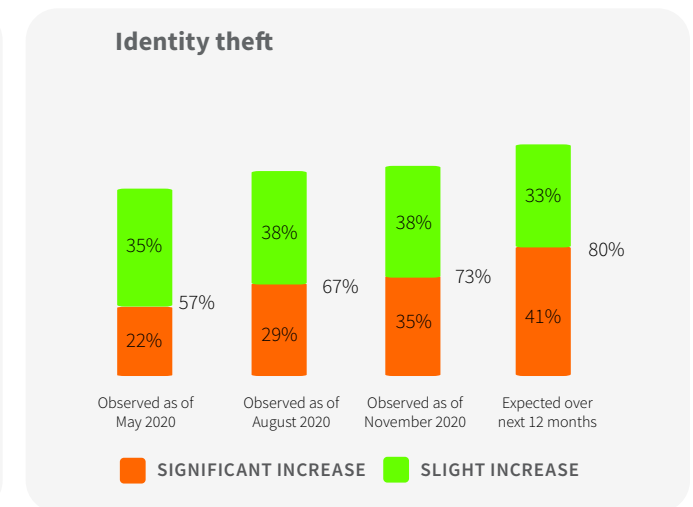
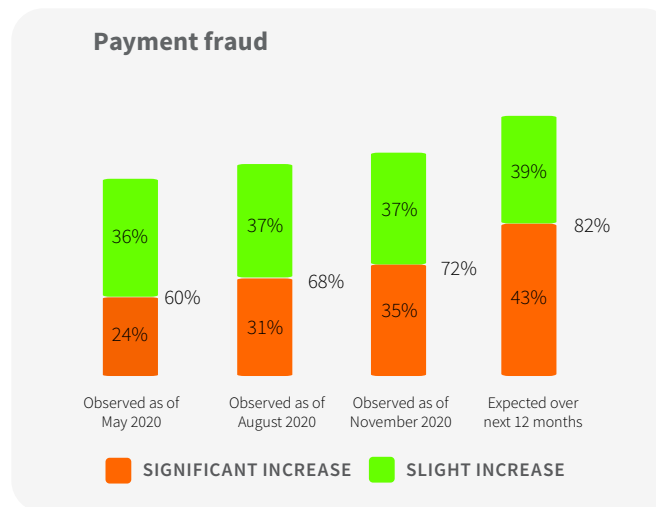
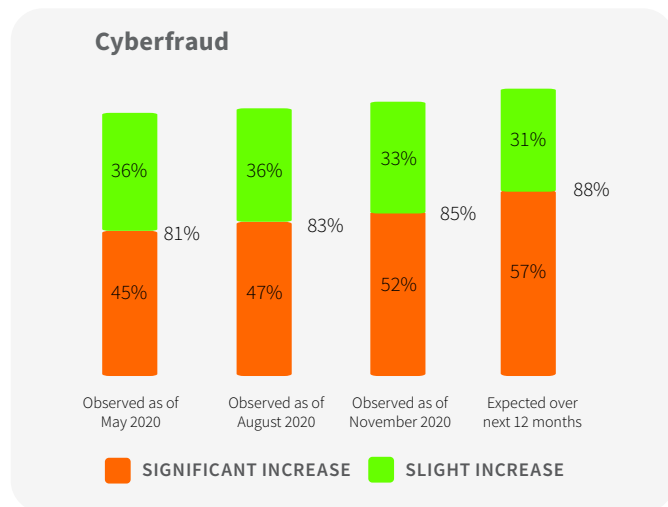
lost and then used by criminals or when a new card is intercepted by fraudsters.

IDENTITY THEFT

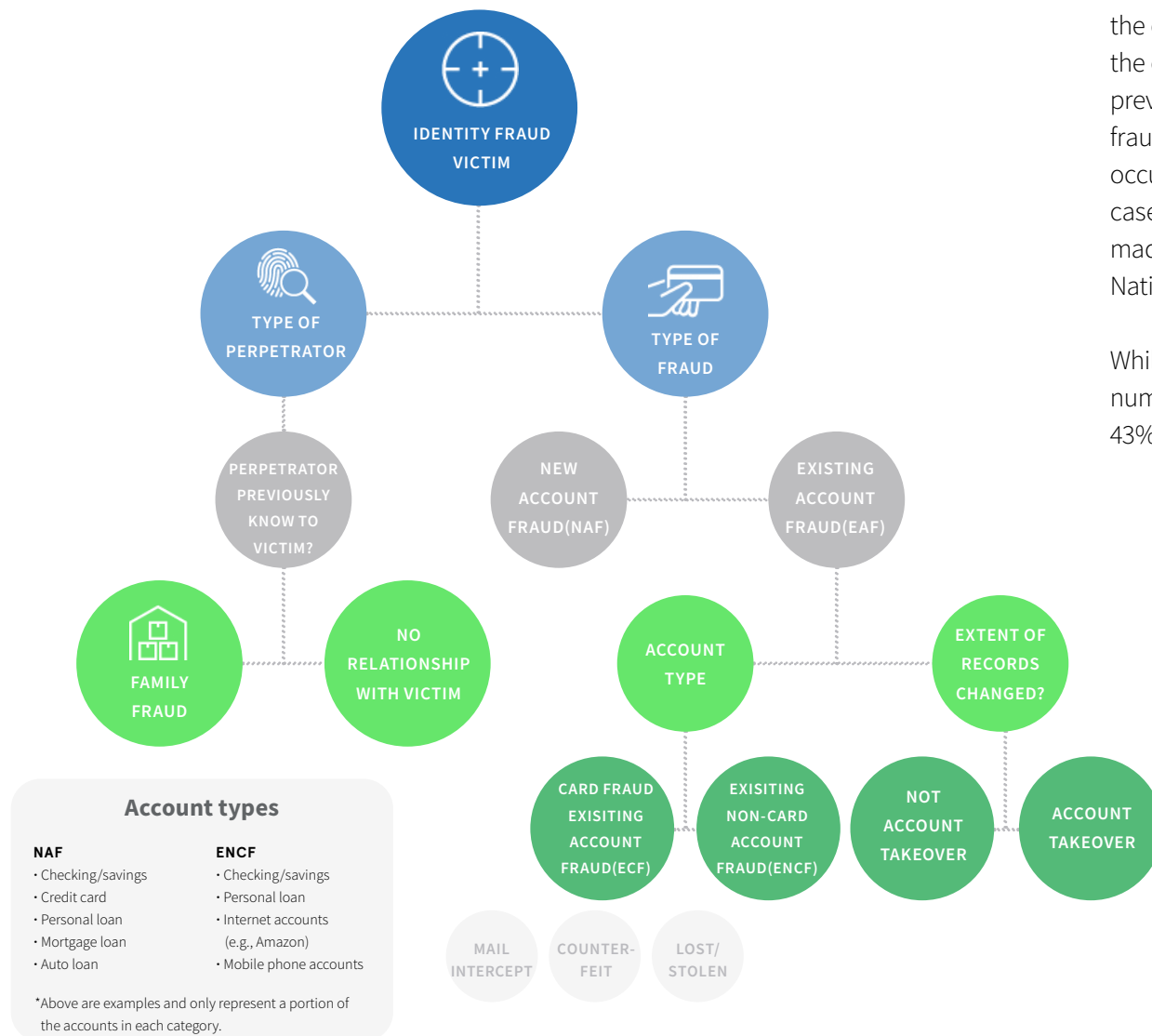
Identity (ID) Theft occurs when cybercriminals use stolen credit cards or card numbers to make purchases that the cardholder never authorized. Last year, Operation Carding Action 2020 disrupted criminal trade in stolen credit card data on the dark web. Together with law enforcement in Italy, Hungary and the UK, Interpol analysed 90.000 pieces of credit card data and prevented around US\$48 million in losses for both consumers and financial

organisations. While fraudsters used to target the elderly, a large number of victims are aged between 41-50 years old, a 43% increase for this age group. A similar pattern can be seen in the US, where the FTC handled 1.6 million fraud reports in 2019. 33% of these were from people between the ages of 20 - 29, while just 13% were from people over 70 years old. In Canada, Equifax revealed a similar trend, with millennials becoming prime fraud targets.

ID theft is best explained in the diagram. This type of fraud results in chargebacks which are filed against the merchant. ID theft is a challenging issue that defrauds

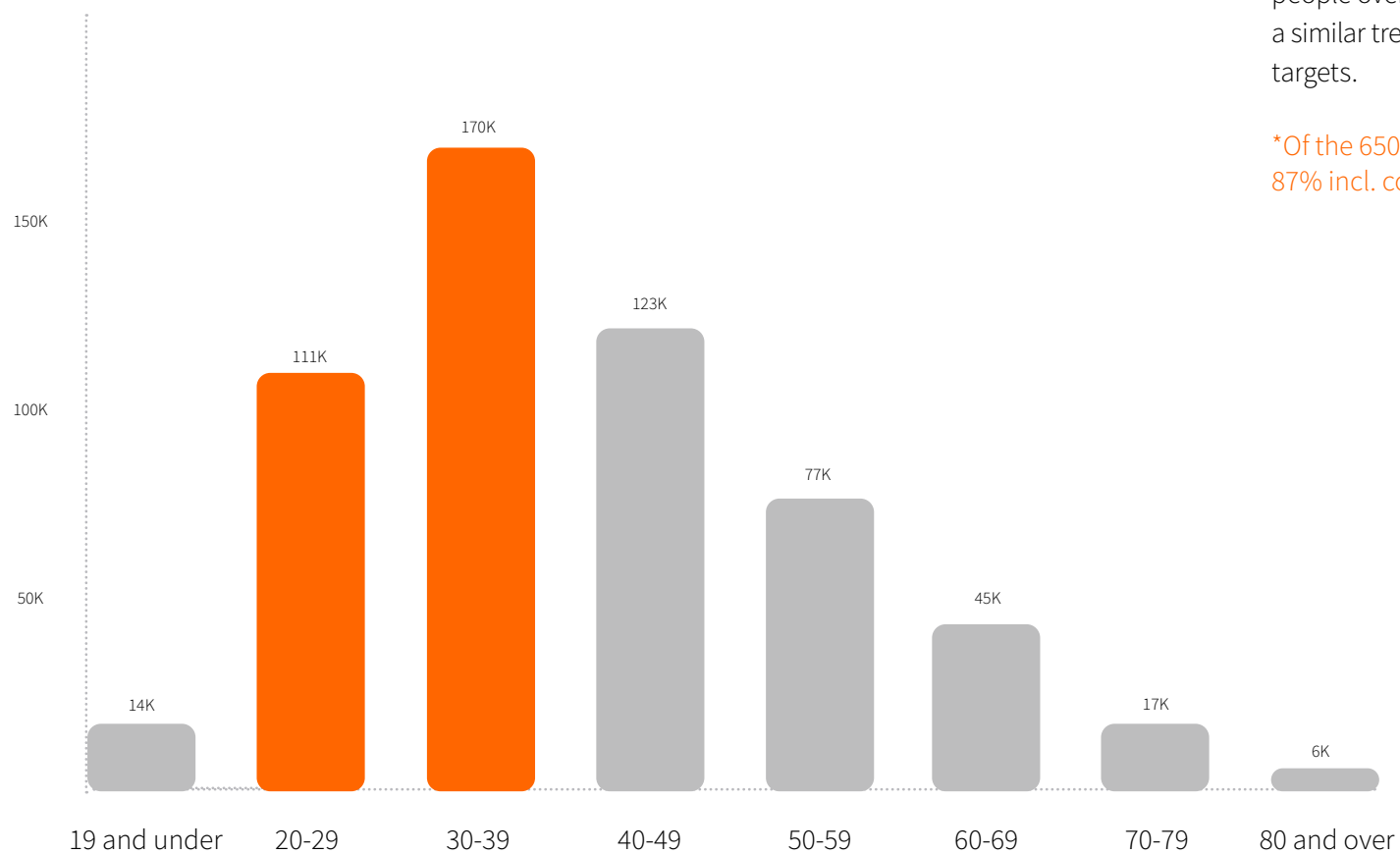


Change in specific fraud risk • Payment Fraud, Cyber Fraud and ID Theft risk increased in the wake of COVID-19 (ACFE)



the card holder and the merchants. Just recently, the organisation that manages the UK's largest fraud prevention database (Cifas), announced that ID fraud reached “epidemic levels” with fraud incidents occurring at a rate of 500 cases per day. Over 130,000 cases of ID theft were reported in 2020. ID fraud cases made up 61% of total cases recorded to the British National Fraud Database.

While fraudsters used to target the elderly, a large number of victims are aged between 41-50 years old, a 43% increase for this age group. A similar pattern can



be seen in the US, where the FTC handled 1.6 million fraud reports in 2019. 33% of these were from people between the ages of 20 - 29, while just 13% were from people over 70 years old. In Canada, Equifax revealed a similar trend, with millennials becoming prime fraud targets.

*Of the 650,572 total identity theft reports in 2019, 87% incl. consumer age information.

➤ Automated transaction monitoring against account takeover

ACCOUNT TAKEOVER

Account takeover occurs when a criminal takes over another person's genuine card account. Based on the card owner's personal information, obtained through data breaches, fraudsters are able to impersonate the genuine cardholder and request a replacement card by falsely reporting theft or loss. If cardholders do not actively monitor their transaction history, account take-over can go unnoticed for quite some

time. Account takeover has increased with 57% over the last months. Javelin Strategy found that 40% of takeovers happen within 24 hours of a criminal's access to a victim's account.

In 2019, account takeovers were 72% up over the previous year. Automated transaction monitoring tools can detect this type of fraud in time.

Javelin Strategy found that 40% of takeovers happen within 24 hours of a criminal's access to a victim's account.



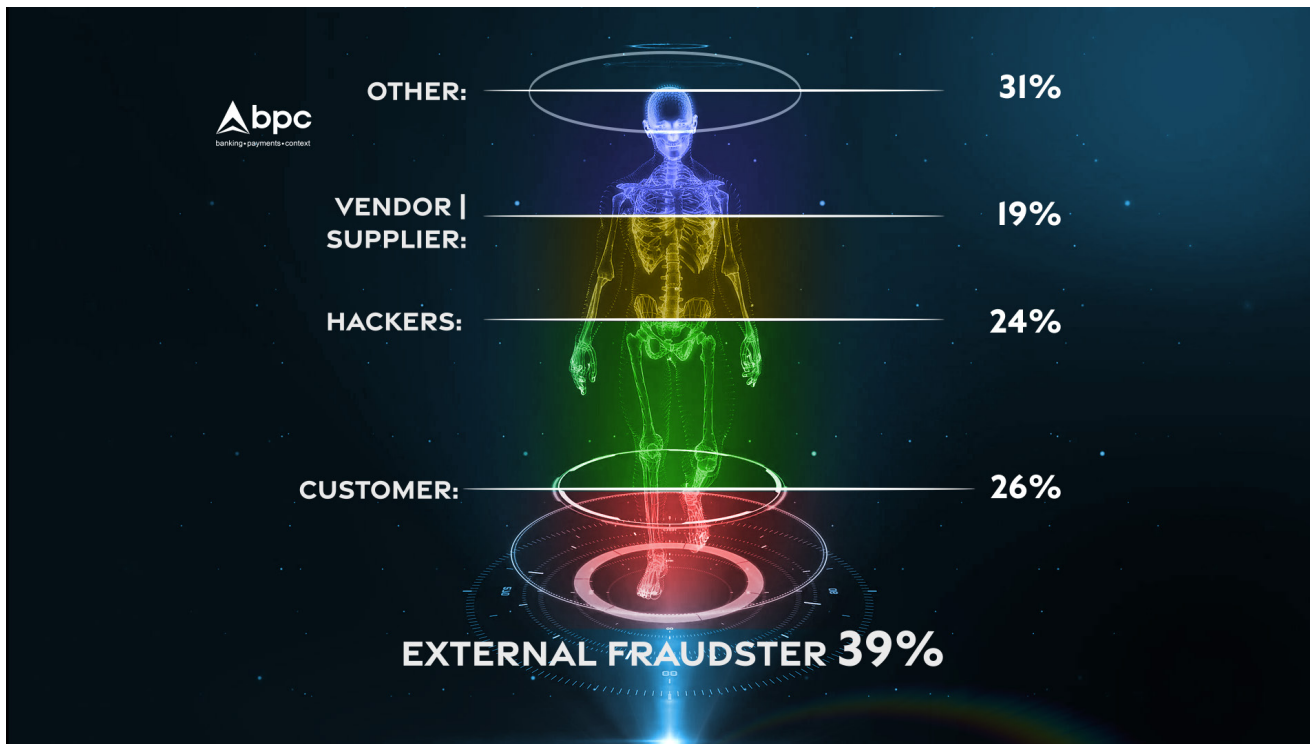
➤ 3 Who is the fraudster?

➤ *The external fraudster*

Hackers, customers, vendors and suppliers represent three quarters of all external fraudsters. Fraudulent customers might submit bad checks or falsified account information for payment, or might attempt to return stolen or knock-off products for a refund. Dishonest vendors might engage in bid-rigging schemes, bill the company for goods or services not provided, or demand bribes from employees.

In addition, organisations also face threats of security breaches and thefts of intellectual property perpetrated by unknown third parties. Other examples of frauds committed by external third-parties include hacking, theft of proprietary information, tax fraud, bankruptcy fraud, insurance fraud, healthcare fraud, and loan fraud.

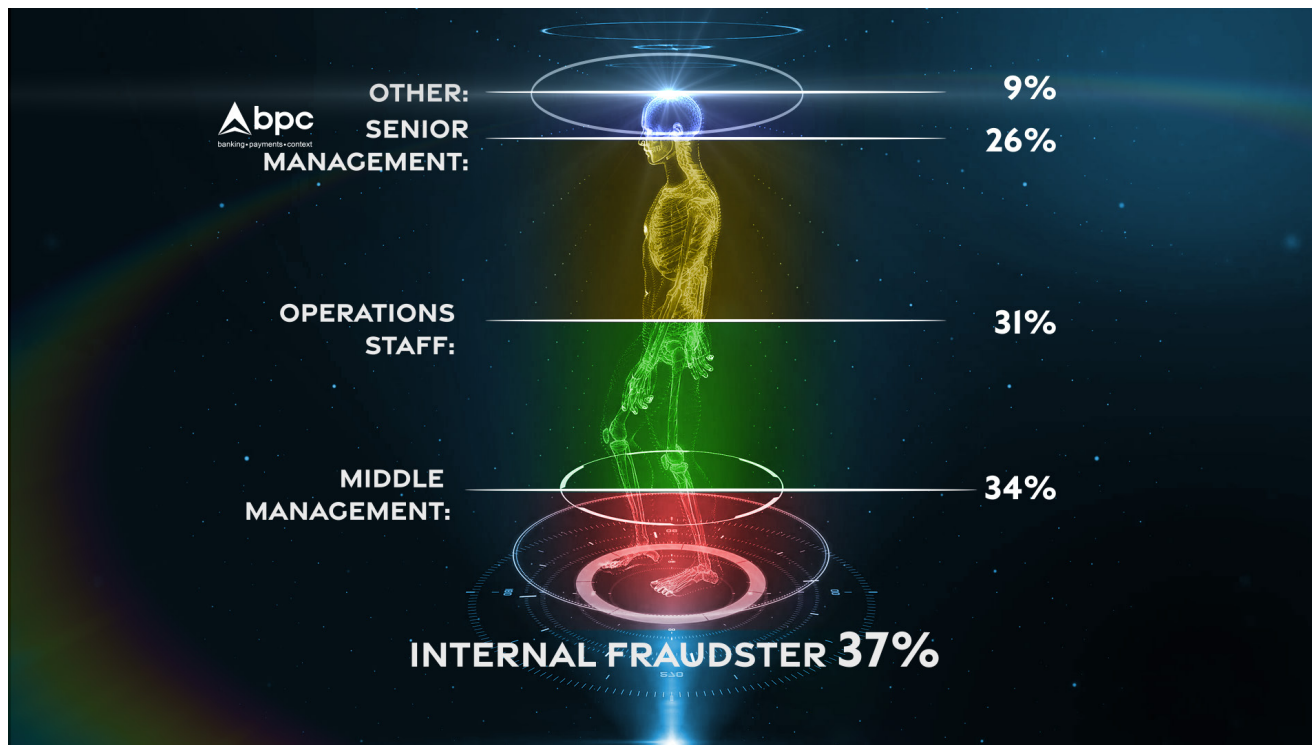
The pandemic has boosted online sales. Companies involved in e-commerce want to “grab the momentum”, but this means they often face supply chain challenges, as a consequence of suddenly increased customer demand. Having been forced to turn to alternative suppliers and delivery companies, businesses may skip due diligence procedures that prevent fraud. This has exposed businesses to increased risk of engaging with fraudulent or inexperienced suppliers, or of employee collusion with third parties. The pandemic also increased business deals between companies and governments. Companies bid for lucrative government contracts and government officials may be corrupt. This increases the risk of bribery, especially in countries where corruption is rampant.



➤ *The internal fraudster*

Internal fraudsters or occupational fraudsters represent a major internal threat for businesses and organisations. According to an extensive survey, conducted by the Association of Certified Fraud Examiners (ACFE), 65% of internal fraudsters are employed by the company, 38% of whom have been with the company for over 6 years. These employees cause twice the amount of average fraud

losses (\$200K). 20% of internal fraudsters work at an executive/C-Level and cause the highest amount of average fraud loss (\$600K). Their authority and the trust they have built inside the company, enables them to override internal controls. Typical fraud loss varies per region, but the overall numbers are estimated to run in the trillions worldwide.



➤ Collusion



COLLUSION

20% of all fraud schemes are the result of a collaboration between internal and external fraudsters. Groups of fraudsters often consist of people both inside and outside the defrauded company. If their schemes results profitable and they are not caught, they will repeat the same fraud scheme and gain considerable profit. The collusion often involves former employees, vendors, suppliers or customers who conspire with a corrupt employee inside the company. This highlights the need for better third-party due diligence.

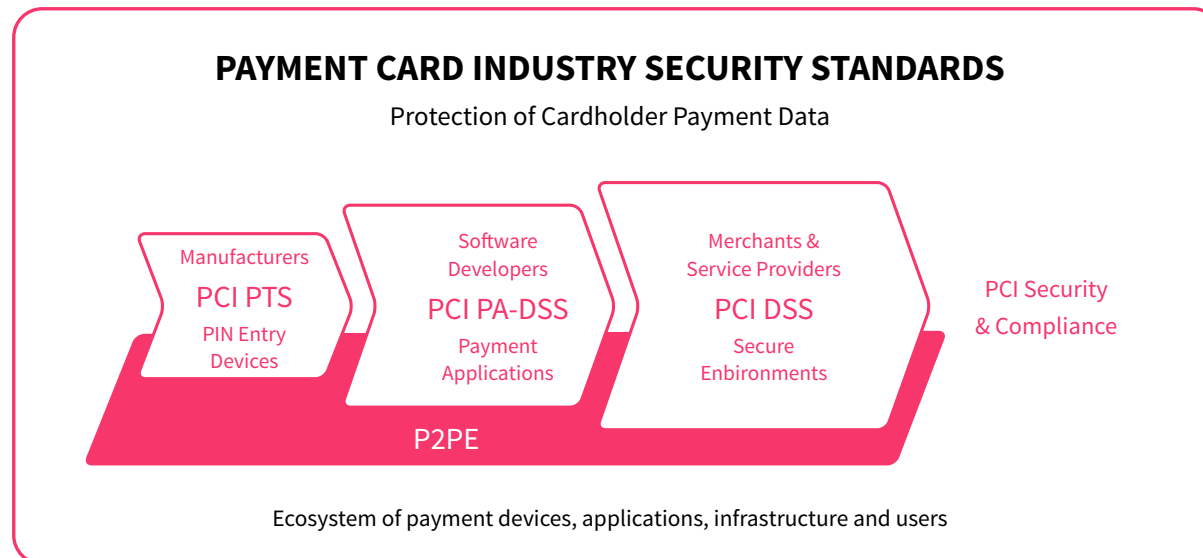


➤ 4 Security, detection and prevention

➤ Legal compliance

LEGAL COMPLIANCE

Financial institutions that handle payment transactions have to comply with the Payment Card Industry Data Security Standard, a set of industry standards as defined by the PCI Security Standards Council. This Council was founded in 2006 by 5 major card schemes: VISA, MasterCard, JCB International, American Express and Discover. Its aim is to provide the global payments industry with periodically updated legal security standards. [The PCI Security Standards Council](#) “helps merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data.”



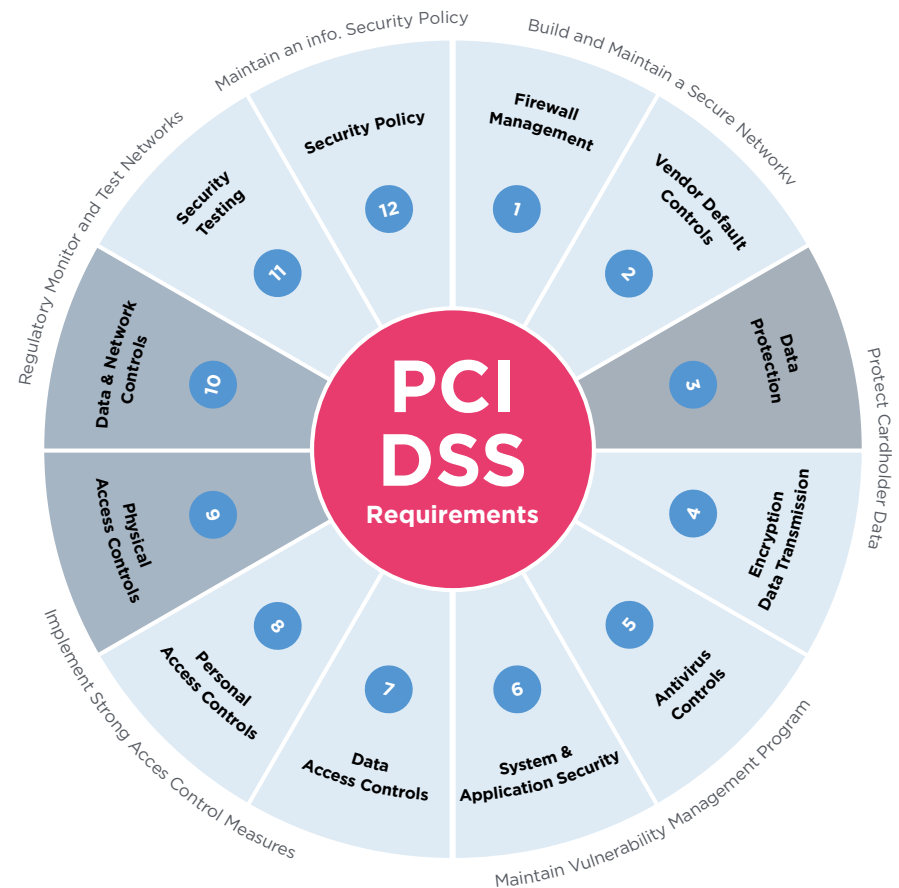
➤ PCI-DSS standards

PAYMENT PROCESSORS ARE REQUIRED TO MEET BASIC PCI-DSS STANDARDS

- Install and maintain a firewall configuration to protect cardholder data
- Don't use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for employees and contractors

Payment service providers and merchants acquirers have to permit periodical regulatory compliance audits. The recent Wirecard scandal shook up

the e-payment industry and has highlighted the fundamental importance of thorough audits. Auditors had given two qualified opinions on the company's audited financial statements; red flags which were largely ignored.



➤ Risk management

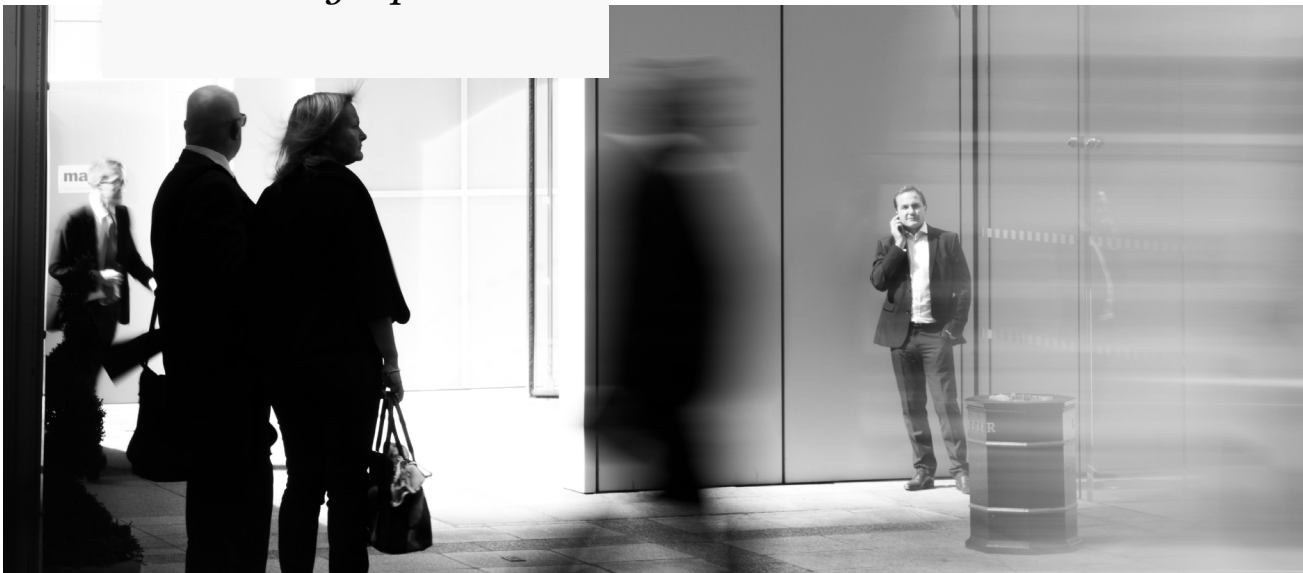
Fraudsters could hide behind the façade of a fancy web shop filled with low-risk products and sell illegal products

There are different categories of risk, each of which require specific detection and prevention strategies. Risk professionals have to be able to detect and prevent:

- Business risk
- Financial risk
- Brand Reputation risk
- Fraud risk
- Chargeback risk
- Money laundering
- Transaction laundering

Fraudsters could hide behind the façade of a fancy web shop filled with low-risk products and sell illegal products and services “in the backyard”. Transaction- and money launderers abuse web shops as a fast way to white-wash criminal income. There are many types of fraud and financial criminals are very good in staying ahead of the game, by inventing increasingly complex fraud schemes. Risk departments have to verify the true nature of the merchant’s business, the identity of the ultimate beneficiary owner, the merchant’s history, his business model and marketing strategy, in order to be able to rule out suspicious activity that requires further investigation.

PSPs or acquirers implement risk management solutions, but due to the growing complexity of having to manage risk across payment multiple channels and in different jurisdictions, these companies often prefer to invest in partnerships with companies that are specialized in multichannel risk management, compliance and fraud prevention. Companies that offer solutions, empowered with the latest technology. According to PwC’s 2020 Global Economic Crime and Fraud Survey, companies with a dedicated fraud prevention program spent 42% less on response and 17% less on remediation costs than companies without integrated risk management programs.



➤ Customer due diligence

CUSTOMER DUE DILIGENCE

Customer and business identification and authentication programs are key to the prevention of financial crimes. Before the start of a relationship between legal entities, it is of crucial importance to know your customer (KYC) or Know Your Business (KYB). Due Diligence procedures are legally required and include screening, identity verification and an in-depth analysis of the risks this business relationship poses to the organisation.

After customer acceptance, risk has to be managed on a continuous base, in order to avoid financial

or reputational damage. This is called ongoing due diligence or ODD. This complex process is partly manual, partly automated, with the help of artificial intelligence (AI), machine learning (ML), device fingerprinting, biometrics and other innovative solutions.

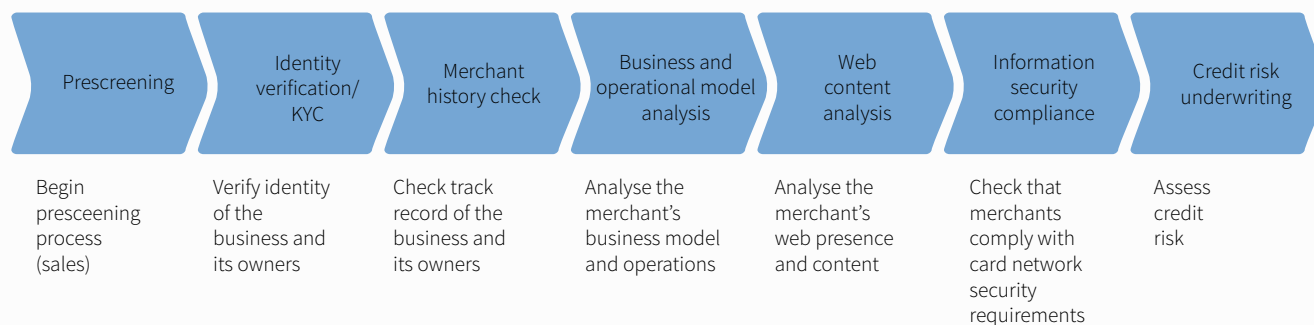
THE INVESTIGATION

Right from the start of the investigation, all relevant risk indicators should be identified and classified. Investigators have to identify primary and secondary risks. Missing crucial indicators could lead to a wrong risk assessment. Fraud risk is only one of many risk categories, as defined by the card associations. The four basic investigation steps consist of:

- In-depth understanding of the business
- Data collection
- Data analysis
- Link analysis

The importance of understanding the true nature of the business, cannot be underestimated. The (high, medium, low) risk of the products and/or services that the merchant offers has to be assessed. What is the company structure, where are its hubs located, what are its principle markets and in which regions? Is all the legally required information present on its website

Onboarding and underwriting process • Aite Group



➤ Risk assessment

and in the presented corporate documentation? It is fundamental to identify the ultimate beneficiary owner (UBO) and all the executives at C-Level.

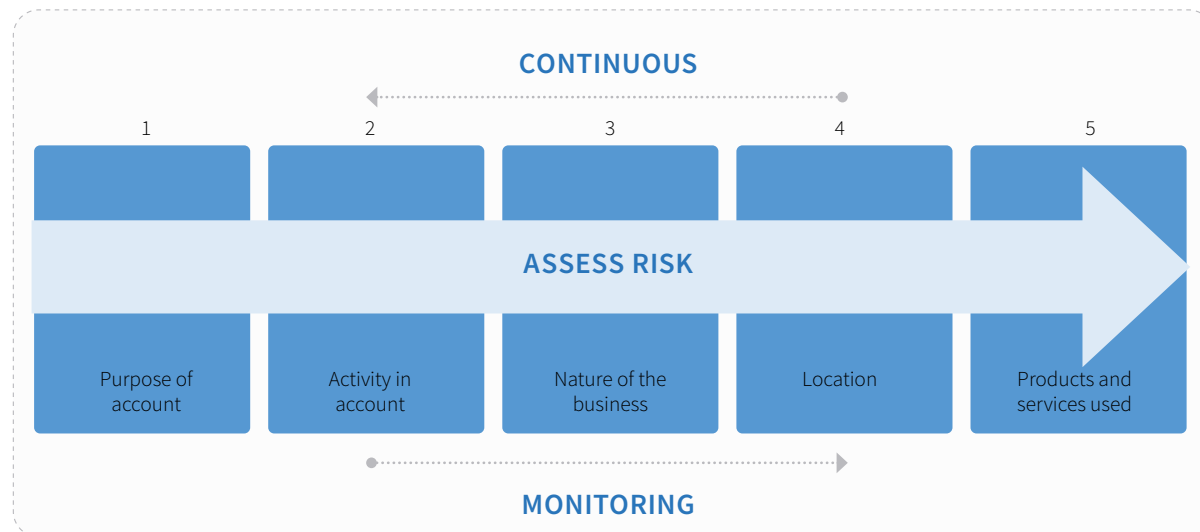
All required data has to be collected and from many different sources. When investigating a web merchant, the data collection phase is quite labor-intensive, especially if the merchant operates across different countries and multiple websites. Examples of investigation strategies for CNP merchant acceptance are described into great detail in a book published by Webshield Ltd.

Once all relevant data is collected, this gathered data has to be analysed. Innovative link analysis solutions reveal hidden connections between legal entities, addresses, business relationships, possible red flags or hits on sanctions lists, which require further investigation. AI and ML algorithms reveal hidden patterns, which could be an indication for suspicious activity. Digital footprints, content on social media, IP localization, are just a few of the many elements that are analysed. This is especially important in a multi-channel payment environment.

Transactions and events, extracted from multiple channels, have to be analysed and monitored to detect unusual patterns.

Machine Learning helps:

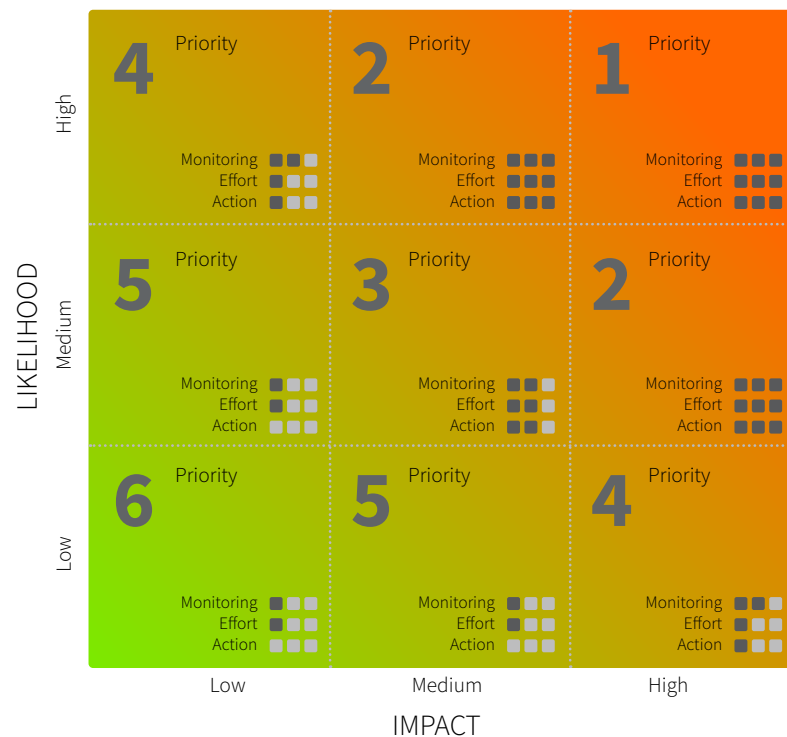
- To build risk and fraud models based on known cases
- Segmenting customers, by detecting KYC and transaction activity
- Predicting and risk scoring of online transaction
- Analysis during their decision making/risk assessment phase
- Operators in daily routines



RISK ASSESSMENT

Risk assessments used to be the result of time-consuming manual information gathering, research and analysis, but these days' underwriters and risk professionals increasingly use automated tools that help them assess risk. Thanks to new technology, Artificial Intelligence empowered rules engines gather and analyse vast amounts of data. Legal entities are automatically screened along sanction lists. Machine Learning considerably reduces false positives.

➤ Calculation of risks by impact and likelihood



False positives are “false alarms” that are frustrating for investigators and for the entity that is mistakenly deemed suspicious. Even worse are false negatives, when criminal business activity goes unnoticed, because fraudulent transactions did not trigger red flags. False negative expose acquirers and the PSPs to serious financial risk and brand reputation damage.

Risk is scored, based on a calculation of risk factors, their impact and on the probability of its occurrence. Transactions are monitored (almost) real-time. Each transaction is validated along a predefined set of business rules, which monitor hundreds of parameters (i.e. location, card transaction history, customer profile, business segment, merchant profile). These rules can be customized according to the company’s ‘risk appetite’ in relationship with the type of merchants in his portfolio.

Statistical Machine Learning improves output and scalability.

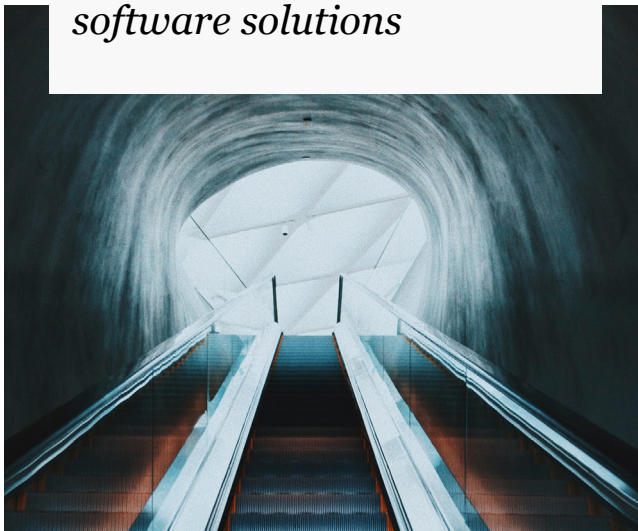
Unusual patterns are immediately detected and analysed. Automated Link Analysis connects the hidden dots that are easily missed through manual analysis. Relationships between legal entities, phone numbers, addresses, UBOs, companies, and other relevant data are automatically uncovered. This allows risk investigators to visualize the connections between large amounts of data that entered into the system. This results in much better and faster decision-making, particularly when investigating highly complex insurance fraud and money laundering schemes.

Device fingerprinting is the collection of a machine’s unique hardware, software and IP location. Browsers collect unique data, so-called digital fingerprints which are left behind on a user’s smartphone or laptop. This tool is especially effective to detect bot attacks synthetic identities, account takeovers, ID theft and CNP fraud, but device fingerprinting has to be part of a holistic risk management strategy.

The same rule applies to biometrics. Biometric authentication verifies the true identity of the person through its unique individual traits (iris, voice, fingerprint, etc.), which makes it a great solution to detect fraudsters who abuse their victim’s ID.

➤ *Fraud prevention*

Fraud prevention is very complex and requires dedicated departments that invest in human expertise and in dedicated software solutions



As millions of online shoppers turn to contactless and alternative payment methods, risk management solutions have to be able to analyse data from multiple channels (i.e. ATM, POS, mPOS, Wallets, etc.). Risk can only be mitigated cost- and time efficiently by integrating high-tech, sophisticated solutions through a holistic strategy.

SANCTION LISTS

All card associations' licensed principal members need to comply with OFAC regulations and local sanction requirements. Merchants, their associated director(s) and UBO(s) have to be screened along sanction lists (i.e. [OFAC](#), Politically Exposed People (PEP) lists), both during the customer acceptance and customer identification phase and after onboarding. This is called enhanced or ongoing due diligence (ODD). Legal entities have to be screened, especially the C-Level executives who run the business, in order to detect fraud, money laundering, transaction laundering or terrorist financing schemes.

CARD ASSOCIATIONS AND REGULATIONS

Principal Members, such as card issuers and acquirers are obliged to follow the rules and regulations of the card associations. Major card associations such as Visa and MasterCard, demand regulatory compliance from their principal members. Violating these rules

and regulations may lead to heavy fines and to [RIS](#) or [SAFE](#) penalties if fraud rates pass thresholds as defined by the card organisations. Besides fines and monitoring.

Programs, the FI may be forced to shut down by Visa or Mastercard. MasterCard's Business Risk Assessment and Mitigation (BRAM) Program and Visa's Global Brand Protection Program (GBPP) are designed to protect card brands and consumers from illegal and/or brand-damaging activity. These programs impose fines on acquiring banks for any detected processing of fraud, illegal activity, or activity that may pose regulatory or reputational risk.

As we have learned in the previous chapters, fraud detection and prevention challenge all stakeholders that are involved in the lucrative e-commerce and payments business. Fraud prevention is very complex and requires dedicated departments that invest in human expertise and in dedicated software solutions, in order to mitigate risk on the long-term. Partnering with a company that offers state-of-the-art risk solutions, empowered with the latest technology, may be a costly short-term investment, but it ultimately saves the organisation long-term expenses on training programs and human resources that are necessary to prevent financial and reputation damage.

➤ 5 Conclusion

➤ Conclusion

Fraud prevention is a challenge for all stakeholders that are involved in the lucrative e-commerce and payments business. Fraudsters target individual consumers, private companies, NGOs and government institutions, causing substantial financial and reputational damage. The 2020 global pandemic has forced countries around the world in lock-down. Millions of consumers made their first online purchase and with many forced to work from home, fraudsters shifted their target, from the elderly to home-bound and digitally active millennials who work, meet, shop, buy and socialize online.

This has exposed the companies and government agencies they work for to increased risk. Home offices are not as secure against cyber-attacks. With millions of consumers forced to buy their groceries, books, electronics, etc on web shops, the amount of online transactions grew and so did fraud. Card-not-present (CNP) fraud is estimated to have increased with 70% since the start of the pandemic.

Card fraud and ID Theft have gone rampant. In 2020, ID fraud cases made up 61% of total cases in the British National Fraud Database. Forced under lock-down, millions around the world socialize and interact online. The US Federal Trade Commission

announced that reported losses through social media fraud scams climbed to nearly \$117M during the first half of 2020. The rise of e-commerce has boosted all fraud schemes which target digital payments, schemes such as transaction laundering and charge-back fraud. “Friendly fraud” has become the most common and costly charge-back fraud scheme.

WHO ARE THESE FRAUDSTERS?

Fraudsters can be divided into external and internal fraudsters, who commit their crimes from within the company they defraud or from the outside, often with the help of a complicit insider. Customer (KYC) and business (KYB) identification and authentication programs are key to the prevention of financial crimes. Due diligence procedures are legally required and include the screening, identity verification and in-depth analysis of all the risks that a new or existing business relationship poses to an organisation.

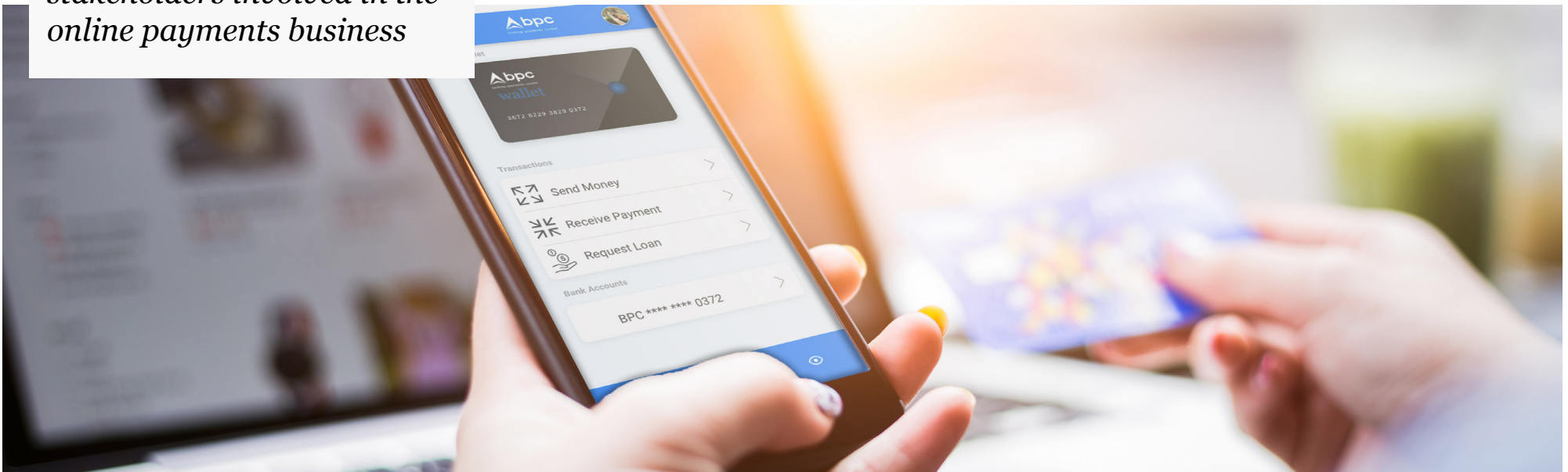
Artificial intelligence and machine learning reveal hidden patterns, which could be a reason for suspicious activity. Transactions and events, extracted from multiple channels, have to be analysed and monitored to detect unusual patterns. Machine Learning also improves speed, output and scalability. Unusual patterns are immediately

➤ Conclusion

Sharing knowledge to raise awareness among all stakeholders involved in the online payments business

detected and analysed. Link analysis connects the hidden dots that are easily missed through manual analysis. Device fingerprinting, IP localization and biometrics have improved risk assessment procedures in customer identification programs. Innovative risk management solutions enable risk managers to analyse data from multiple channels (i.e. ATM, POS, mPOS, Wallets, etc.). Risk can only be mitigated cost- and time efficiently by integrating high-tech, sophisticated solutions through a holistic strategy. Card issuers, PSPs and merchant acquirers are obliged to follow the rules and regulations of the

card associations. Major card associations such as Visa and MasterCard, demand regulatory compliance from their principal members. Violating these rules and regulations may lead to heavy fines, penalties and termination. The importance of implementing intelligent, innovative risk management and fraud prevention programs cannot be overestimated. With this guide, BPC aims to share its knowledge of fraud prevention with its readers in order to raise awareness among all stakeholders involved in the online payments business.



➤ 6 Use cases

➤ *DSK Bank, Bulgaria*

Uncovering fraudulent merchants through smart insights

THE BANK

DSK Bank is Bulgaria's leading commercial bank. It is a member of OTP Group (Hungary) and owned by OTP Bank. In 2019, DSK Bank finalised the acquisition of Societe Generale Expressbank and its subsidiaries in Bulgaria. The bank addresses a large number of segments, from mass affluent consumers to corporates and is also the preferred bank for students due to its innovative services.

THE CHALLENGE

DSK Bank embarked on an ambitious transformation programme to replace a legacy system which was constraining its teams' ability to operate efficiently and manage their customers' channels, card and customer payment experience.

THE SOLUTION

The bank initially selected BPC's SmartVista solution to manage its card lifestyle. Based on this experience it decided to extend the usage of SmartVista to prevent fraud attacks from card issuing to the acceptance of payment methods, providing full support and tracking capabilities for fraudulent activities within the bank's environment.

THE RESULT

The bank was able to take full control of its risk management strategy. BPC teams helped configure the initial rules while the bank defined 26 different scenarios for screening transactions and touchpoints in real time. SmartVista has helped uncover over 600 fraudulent merchant locations and prevent more than 4000 attacks using counterfeit and stolen cards, reducing financial losses while increasing efficiency within just a few months. The bank has gained full control over scenarios and rules definition and can act in real time without the need for external technical expertise.



➤ TymeBank, South Africa

THE BANK

TymeBank is South Africa's newest digital bank and a model for neobanks worldwide with its fast growth path. It has signed up 2.5 million customers in just over a year thanks to a hybrid model that combines mobile and self-service kiosk banking.

THE CHALLENGE

The bank was launching from the ground up, leveraging instant distribution of debit cards from self-service kiosks. With card usage expected to increase exponentially, the bank needed to ensure it was equipped with the best tools to protect its customers and was going to market with a service that was safe and secure.

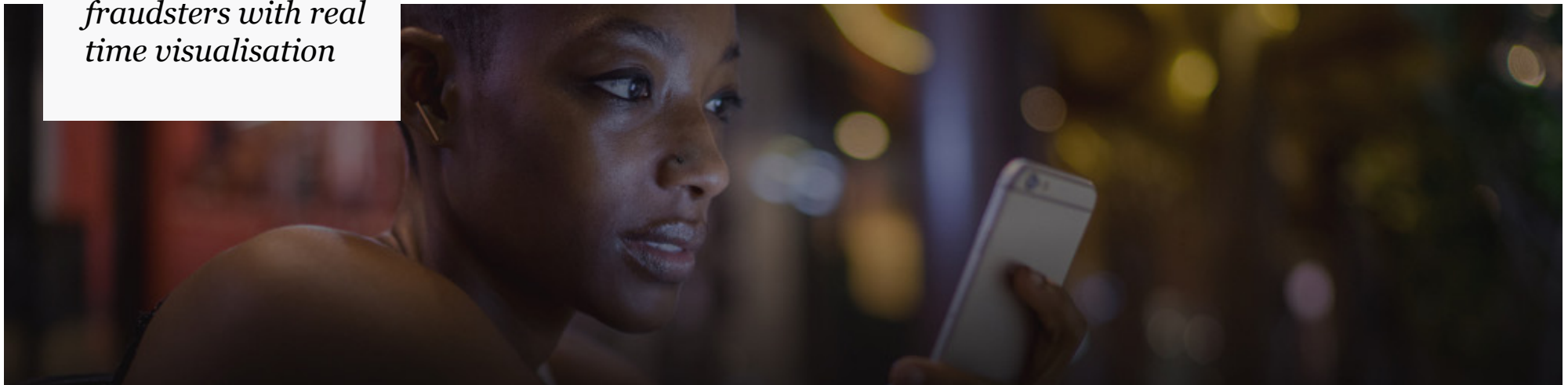
THE SOLUTION

TymeBank selected BPC's SmartVista for its entire payment experience from the issuance of cards to the acceptance of payments. It also adopted SmartVista's fraud solution to strengthen its card-present fraud prevention strategy.

THE RESULT

TymeBank's risk and fraud prevention teams have the freedom to configure their own rules to suit bank policy without the need for external technical knowledge. The dashboard for rules visualisation, testing of the rules functionality, and real time tracking are all helping prevent fraudulent activity.

*Keeping ahead
of sophisticated
fraudsters with real
time visualisation*



➤ 7 SmartVista Fraud Management Solution

➤ *SmartVista Fraud Management Solution*

BPC's Fraud Management solution helps issuers, acquirers and others detect and prevent fraud across all payment channels, in real-time. The SmartVista Fraud Management solution covers real-time transaction monitoring and allows performing statistics profiling on any level – card, terminal, merchant or device.

SmartVista Fraud management comes with a powerful analytical tool and a robust business-driven rules engine. Each transaction is validated against a set of user defined business rules, which can monitor hundreds of parameters – ranging from simple checks such as transaction location to more sophisticated validations based on the card's historic transaction profile.

Powered by Machine Learning and Neuro Network Model, SmartVista Fraud Management solution helps demystify complex data to enable a smart and safe payments ecosystem for financial institutions and their customers.

The solution can be deployed as a standalone module or as a service through BPC's Global Processing Centre, Radar Payments.





➤ About

ABOUT BPC

Founded in 1996, Banking, Payments: Context is what defines BPC. The company has transformed over the years to deliver innovative and relevant solutions which fit today's consumer lifestyle when banking, shopping or moving in both urban and rural areas, bridging real life and the digital world. With 280 customers across 90 countries globally, BPC collaborates with all ecosystem players from tier one banks to neobanks, payment service providers (PSPs) to large processors, ecommerce giants to start-up merchants, and government bodies to local hail riding companies. BPC's SmartVista suite comprises cutting-edge banking, commerce and mobility solutions including digital banking, ATM & switching, payments processing, card and fraud management, financial inclusion, merchant portals, transport, and smart cities solutions. www.bpcbt.com



ABOUT RADAR PAYMENTS

Radar Payments is a leading innovative payment processing provider dedicated to financial institutions, including payment service providers (PSPs), banks, acquirers, issuers, and fintechs. It offers advisory services and a one-stop platform for end-to-end omnichannel processing, enabling the acceptance of most of the widely adopted payment methods, delivered on a PaaS, SaaS, or fully managed service model. Built using BPC's SmartVista, an industry-recognised payment solution, the Radar Payments platform delivers scalability, resilience, performance, and unparalleled security. Radar Payments is fully owned by BPC and blends BPC's 25 years of expertise in payments with the fintech world – using the latest digital technologies to create innovative customer payment experiences.

www.radarpayments.com



➤ More information



Do you need better fraud protection for your financial institution?
Talk to our team, we can help from ideation to go live and share invaluable experience.
info@bpcbt.com

BPC Headquarters

Neuhofstrasse 5a,
6340, Baar
Switzerland

www.bpcbt.com