Guide

The Anatomy of the New Fraudster

2024

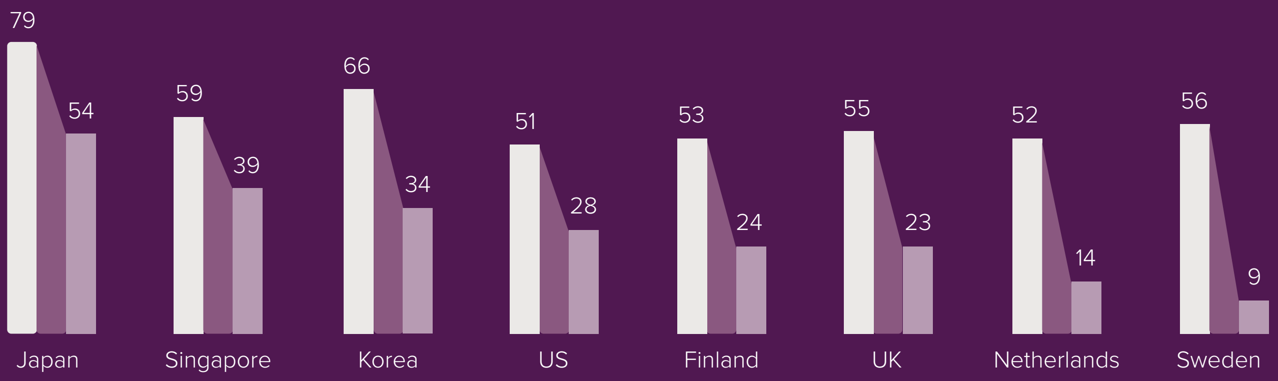
Contents

The Fraud Landscape in 2024

The global payments sector represents substantial financial transactions and associated revenues. According to McKinsey's Global Payments Report for 2023, payments revenues experienced an 11% growth in 2022, marking the second consecutive year of double-digit growth, reaching a record high of over $2.2 trillion. This growth trajectory is anticipated to persist, with projections indicating a surpassing of $3 trillion by 2027. Global Cards and Payments (October 2023) reports that global card purchase volume has already reached $42.7 trillion and is forecasted to escalate to $63.5 trillion by 2028.

Around the world, people's shopping and payment 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 LexisNexis[1], the global payments market is estimated to be worth $2.9 trillion by 2030 but will lose $274.1 billion in 2023, up from $213.9 billion in 2020, in total fraud. The payment business faces a sharp increase in card fraud, particularly in the Card-not-Present (CNP) space. CNP Fraud increased significantly over recent years and according to the latest Nilson report, global card fraud losses exceeded $32 billion in 2021.



Mature markets

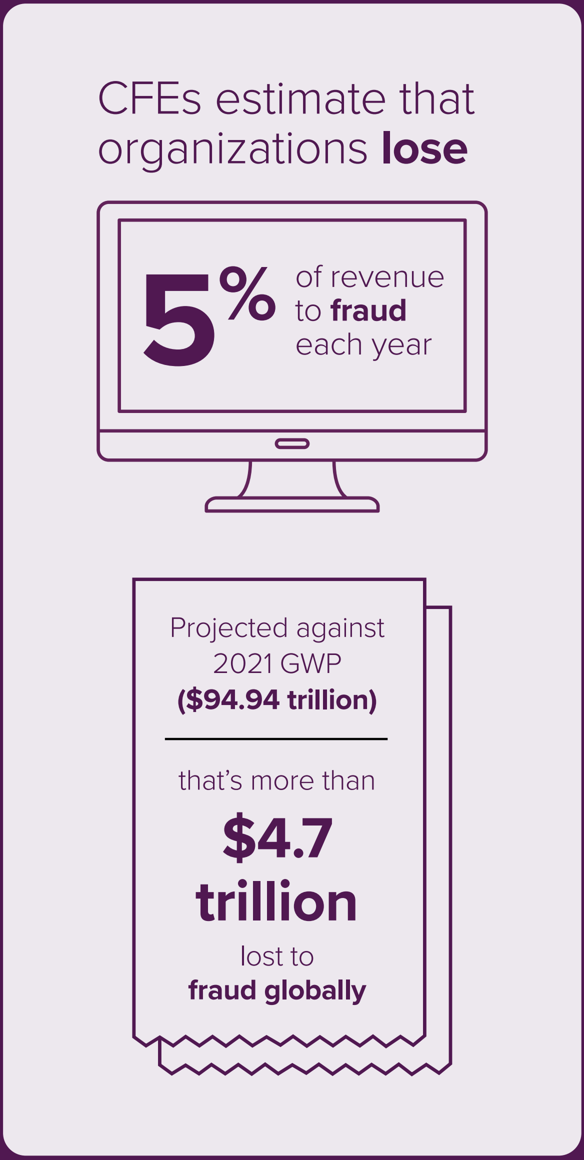
Cashless Payment in Mature Markets (McKinsey, 2020)

In 2021, ACAMS, in their whitepaper titled “The Convergence of Cyber, Fraud, and AML,” forecasted that cybercrime damages would reach $6 trillion annually by that year’s end. This projection indicated a historic shift in economic wealth and highlighted cybercrime’s surpassing profitability compared to the global drug trade. In essence, cybercrime costs outweighed global payments revenue threefold. Furthermore, the “High Stakes of Innovation: Attack Trends in Financial Services” report by UK Finance in October 2023 revealed a significant surge in web application and API attacks, with a 119% year-over-year increase between Q2 2022 and Q2 2023, totalling 1 billion attacks. In the financial services sector alone, these attacks surged by 65%, amounting to 9 billion incidents within 18 months. Additionally, there were 1.1 trillion recorded instances of “malicious bot requests.”

In terms of fraud alone, the Association of Certified Fraud Examiners (ACFE) reported losses of USD 4.7 trillion in their “Occupational Fraud 2022: A Report to the Nations.” This sum represented the majority of losses attributed to cybercrime.

Following that, in 2023, the “Fraud & Financial Crime” magazine by Raconteur highlighted that the UK has become a focal point for international financial crime. The severity of this issue prompted the government to officially classify fraud as a national security threat, a decision announced recently. This move aligns with the advocacy of UK Finance, the trade body representing the financial services sector, which had been pushing for such recognition since September 2021.

There should be no doubt that despite the successes in improving cybersecurity, fraud detection, AML procedures, and customer education remain a massive, massive problem.


CFEs estimate that organizations **lose**

5% of revenue to **fraud** each year

Projected against 2021 GWP **($94.94 trillion)**

that’s more than **$4.7 trillion** lost to **fraud globally**

Source: Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations

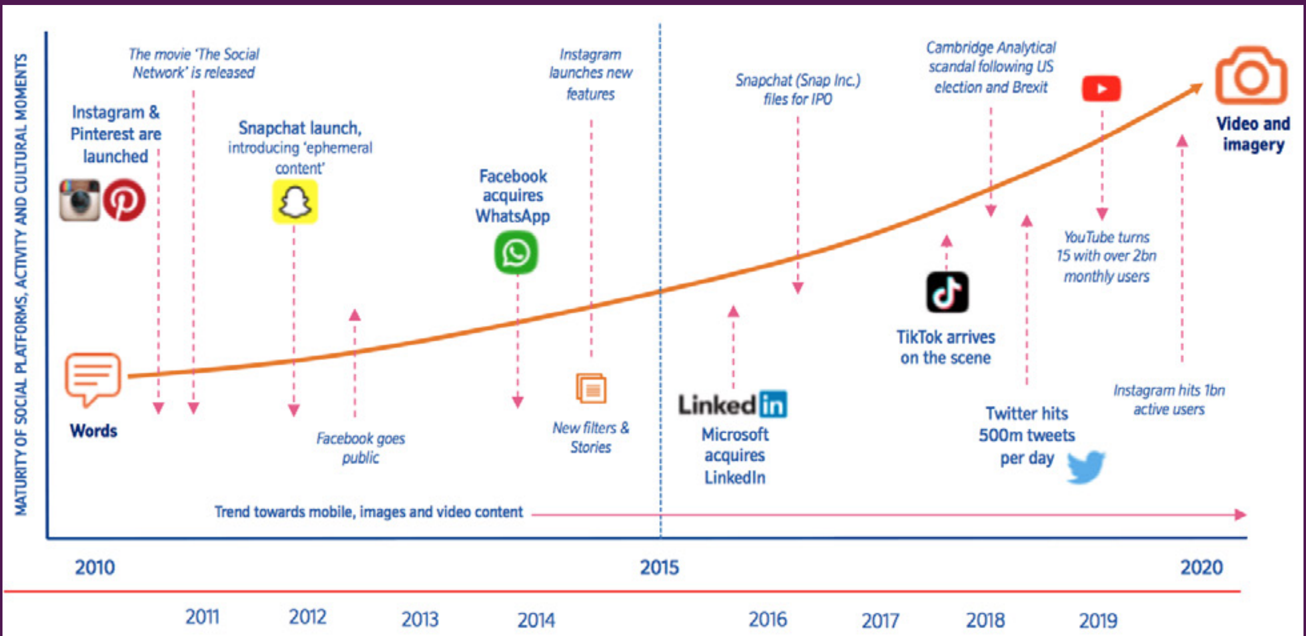
[1] Lexis Nexis, "Key Trends that are Shaping the Fraud and Identity Landscape" (2023).

Fraud Goes Digital

We are witnessing a shift towards digital and online methods, driven by the advent of the Internet, the expansion of social media platforms, and advancements in mobile technology. Financial institutions have recognised this trend as an opportunity to reduce costs associated with staffing and physical premises, while embracing automation, expanding service offerings, and optimising operations. Banks, in particular, have sought to accelerate the transition away from traditional cash-based transactions.

The pace of this transition accelerated further after the pandemic, compelling even those with limited digital literacy to embrace digital facilities for various transactions, such as online shopping, home deliveries, and remote work. While some activities reverted to pre-pandemic norms following the easing of restrictions, many aspects of daily life remain fundamentally changed to digital.

The way transactions are conducted has undergone a complete transformation, bolstered by the popularisation of instant payment solutions. Consequently, the digital economy has firmly entrenched itself in digital commerce. This evolution has been accompanied by the rise of

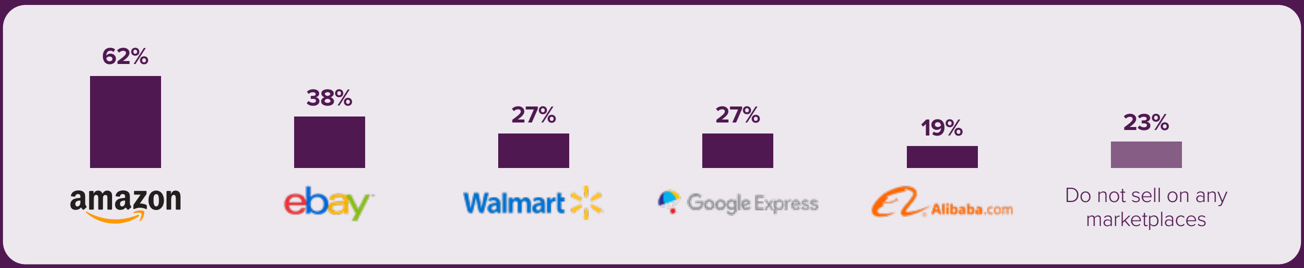

MATURITY OF SOCIAL PLATFORMS, ACTIVITY AND CULTURAL MOMENTS
The movie 'The Social Network' is released
Instagram & Pinterest are launched
Snapchat launch, introducing 'ephemeral content'
Facebook acquires WhatsApp
Instagram launches new features
Snapchat (Snap Inc.) files for IPO
Cambridge Analytical scandal following US election and Brexit
Video and imagery
YouTube turns 15 with over 2bn monthly users
TikTok arrives on the scene
Words
Facebook goes public
New filters & Stories
Linked in
Microsoft acquires LinkedIn
Twitter hits 500m tweets per day
Instagram hits 1bn active users
Trend towards mobile, images and video content
2010
2015
2020
2011
2012
2013
2014
2016
2017
2018
2019

Source: Smart Insights, Social commerce 2023 trends and tactics, February 2023 social commerce, where transactions are conducted through social channels. Newer entrants like TikTok have advanced the trend of social commerce even further. Moreover, innovations in one-to-one communication have emerged through the development of messenger apps such as WeChat, WhatsApp, Instagram, and Facebook Messenger. These platforms have expanded the scope of social commerce by providing users with seamless communication and transactional capabilities within a single interface.

Social commerce involves the direct sale of products within social media networks, enabling users to complete purchases directly within the platform they are currently engaged with, rather than redirecting them to an external online store. This seamless integration streamlines the purchasing process for users, allowing them to conduct transactions without leaving the social media environment.

A significant majority of merchants, accounting for over three-quarters (77%), now leverage third-party marketplaces like Amazon, eBay, and Alibaba to sell their products and services, underscoring the prevalence and importance of online retail platforms in today's commerce landscape.

As cash continues to be displaced, the rise in instant payments and mobile – especially mobile payments and wallets – will continue to accelerate, with electronic payments outpacing general payments revenue.



Global Trends

The financial sector is increasingly confronted with sophisticated fraud schemes that evolve in tandem with technological advancements in Information and Communications Technology (ICT) and the Internet of Things (IoT). This evolution presents substantial challenges not only to emerging fintech startups but also to established banking institutions. As these technologies continue to advance, they open new avenues for fraudsters to exploit, necessitating constant vigilance and innovation in fraud prevention and detection strategies. This dynamic landscape underscores the need for the financial industry to adapt rapidly to protect against the continually changing tactics employed by fraudsters.

Generative AI – a double-edged sword

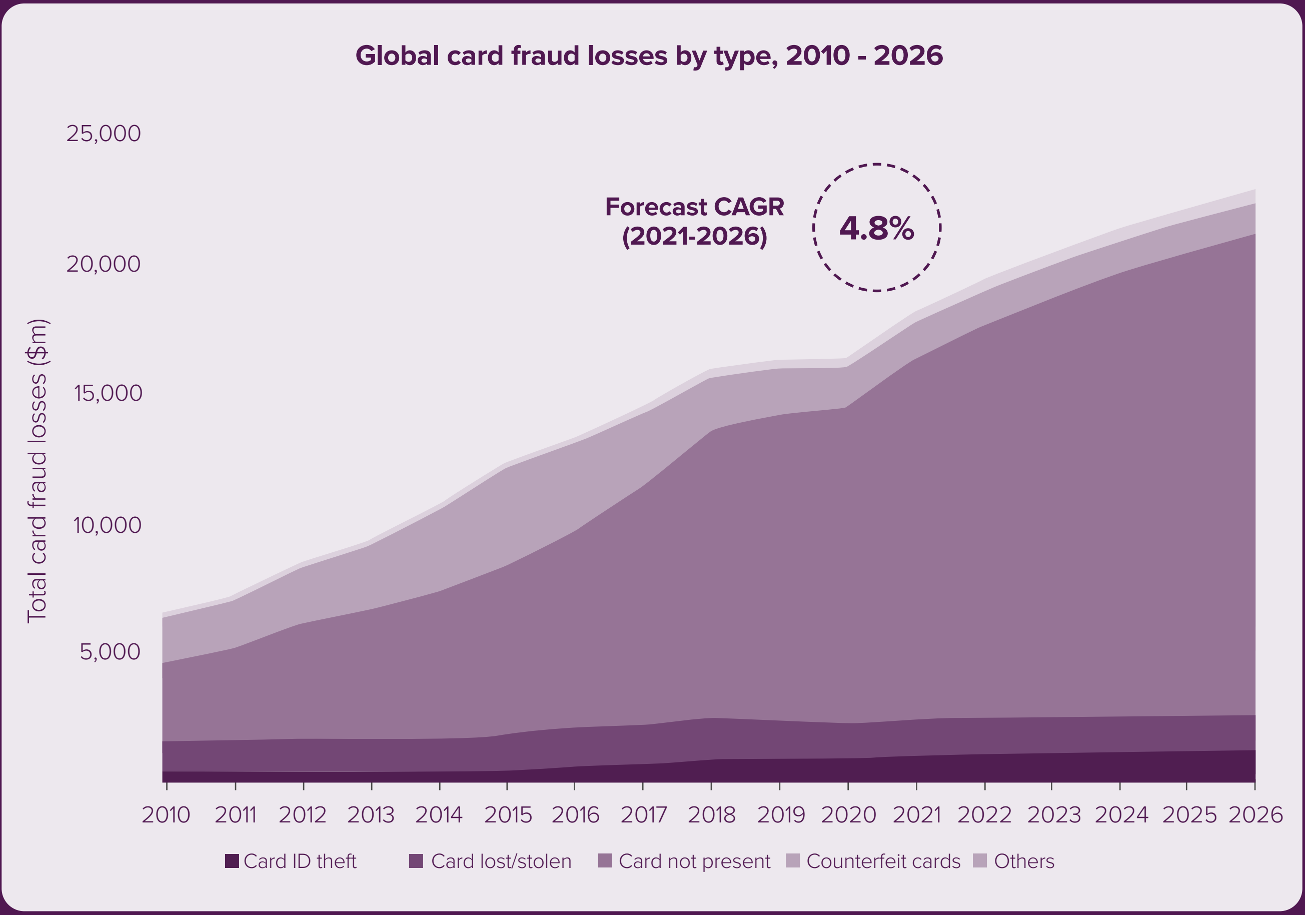
The introduction of Generative AI (GenAI) in 2023-2024 serves as a dual-edged sword in the domain of fraud. While offering a multitude of positive uses, GenAI has also facilitated the creation of sophisticated fraudulent activities. Utilising GenAI, fraudsters can now effortlessly craft synthetic identities and produce deepfakes. This technology enables the generation of convincingly authentic personal information, such as names, social security numbers, and birthdates, culminating in the formation of entirely fictitious identities. These manufactured identities are then employed to unlawfully secure credit cards, loans, and other financial services, often eluding conventional verification processes and leading to considerable losses and security compromises for financial institutions.

Deepfakes, a notable application of GenAI in financial fraud, involve the fabrication of audio or visual content to impersonate significant figures, such as senior executives or clients, for engaging in unauthorised transactions or accessing sensitive information. These advanced fraudulent tactics can easily mislead employees and circumvent established security measures, thus posing grave threats to the financial sector's integrity and security.

Digitalisation and the escalation of fraud

The rise in fraud is not just a consequence of innovation but also the result of increased standardisation and digitalisation, which have expanded the landscape of vulnerabilities. Digital platforms contribute to a significant 61% of global fraud losses, with e-commerce and Card Not Present (CNP) transactions being the major areas of concern. The growth of CNP fraud is expected to continue alongside the expansion of e-commerce, with social engineering tactics becoming increasingly prevalent[2].

[2] Globaldata, "Trends in Payment Fraud" (February 2023)



Source: Globaldata, Trends in Payment Fraud, February 2023

Emergence of next-generation frauds

The digital landscape is witnessing the emergence of sophisticated fraud tactics such as phishing, pharming, and whaling attacks, which continue to dominate as the primary fraudulent activities among merchants globally. Phishing remains the leading method of attack across North America, Europe, and the Asia-Pacific region. Meanwhile, in Latin America, card testing has become the foremost type of fraud. Additionally, merchants are increasingly experiencing the impact of friendly fraud, highlighting a shift towards more sophisticated and diverse fraud strategies in 2023.

Fraud becomes more personalised

Financial institutions have been implementing advanced authentication technologies to curb unauthorised fraud, yet fraudsters are increasingly turning to social engineering scams to coax customers into authorising payments[3]. The European Payments Council's "2022 Payment Threats and Fraud Trends Report" highlights a significant shift from malware to social engineering as the main focus of cybercriminal activities. The rise of social engineering tactics, such as phishing, often coupled with malware, targets a wide audience including consumers, retailers,

[3] NICE Actimize's "2023 Fraud Insights Report,"

Top 5 Attacks By Region

	N.America (n=259)	**Europe** (n=164)	**APAC** (n=112)	**LATAM** (n=84)
1	Phishing/ Pharming/ Whaling	Phishing/ Pharming/ Whaling ↑	Phishing/ Pharming/ Whaling ↑	Card Testing
2	Card Testing	First-Party Misuse	Identity Theft	Coupon/ Discount/ Refund Abuse
3	First-Party Misuse	Identity Theft	Loyalty Fraud	Phishing/ Pharming/ Whaling
4	Identity Theft	Coupon/ Discount/ Refund Abuse	First-Party Misuse	Account Takeover
5	Coupon/ Discount/ Refund Abuse	Card Testing ↑	Card Testing	Identity Theft

Source: Globaldata, Trends in Payment Fraud, February 2023

SMEs, company executives, employees, financial institutions, and payment infrastructures. Moreover, ransomware has become the most significant cyber threat, surpassing traditional banking Trojans in profitability for attackers.

Instant payments, instant fraud

Authorised push-payment (APP) fraud poses a significant challenge as fraudsters manipulate victims into authorising payments under false pretences, including investment and romance scams. UK Finance reports a staggering loss of half a billion GBP to APP fraud in 2023 alone, highlighting the varied tactics employed by criminals, from investment scams advertised on search engines and social media to purchase scams on online platforms. Detecting authorised payments fraud is particularly difficult because, unlike unauthorised payments fraud or account takeover attempts that might trigger alerts due to suspicious activities or unusual transaction patterns, authorised payments fraud involves legitimate users making the payments themselves. This creates a significant challenge for advanced fraud controls and monitoring tools in identifying anomalies in transaction behaviour.

Chapter 01

Fraud Targets

01

Fraudsters have shifted their modus operandi from defrauding elderly consumers to targeting millennials. Millennials spend hours on the internet; studying, teleworking, surfing, shopping, and buying products and services. This makes them easy targets for cybercriminals engaged in ID theft and other fraud schemes, which will be discussed in the next chapter.

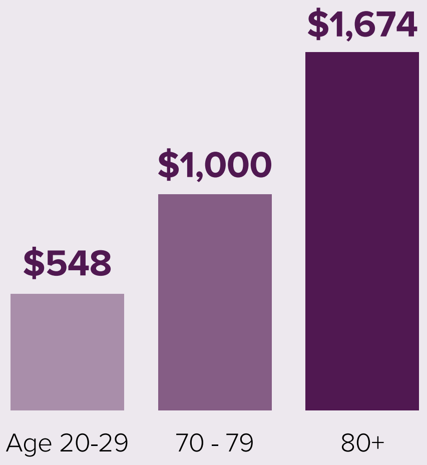
According to the FTC's "2022 Consumer Sentinel Network Data Book" from February 2023, individuals aged 20-29 reported experiencing financial losses due to fraud in 43% of the reports filed with the FTC. In comparison, individuals aged 70-79 reported losses in 23% of their reports, while those aged 80 and over reported losses in 22% of their reports. Despite a lower incidence rate among older age groups, those aged 70 and older reported significantly higher median losses when they fell victim to fraud compared to other age groups. This disparity highlights the heightened vulnerability of older individuals to substantial financial losses resulting from fraudulent activities.

Younger people reported losing money to fraud **more often than older people.**

43%
Age 20-29

23%
Age 70-79

But when people aged 70+ had a loss, **the median loss was much higher.**

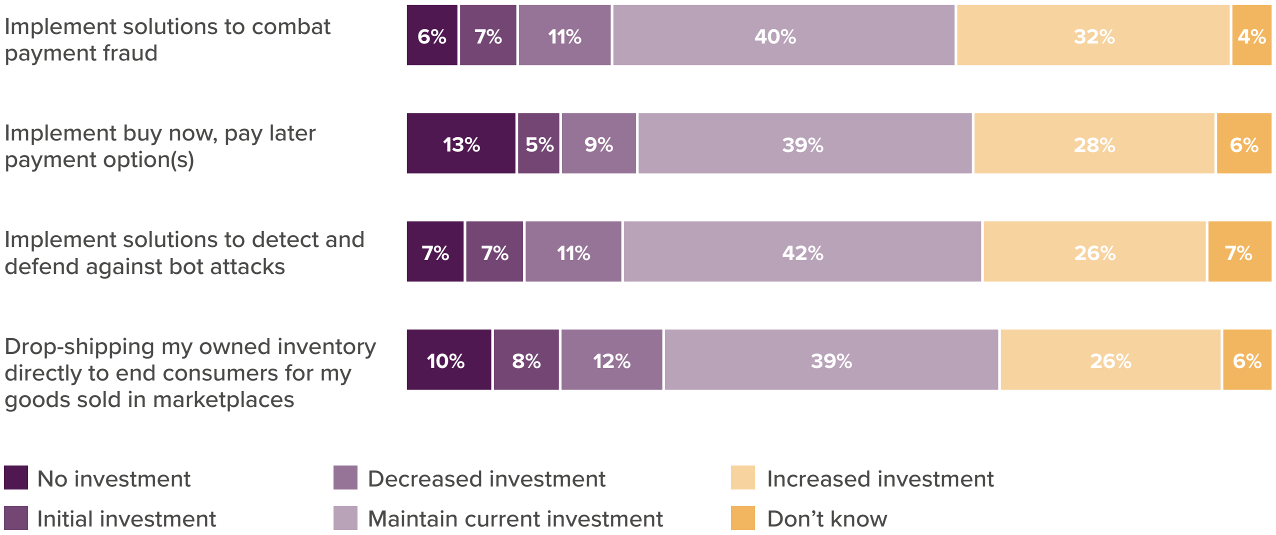


Source: FTC, 2022 Consumer Sentinel Network Data Book, February 2023

Private companies are fraudsters' preferred targets. The Association of Certified Fraud Examiners (ACFE)'s "Occupational Fraud: A Report to the Nations" (2022) reveals that 44% of reported fraud cases involve private companies, and these targets suffer the highest amount of financial loss. Private SMEs have always been lucrative targets for elaborate fraud schemes, especially financial institutions. Exploiting "weak links" such as corruptible employees, or persuading untrained personnel 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.

According to a Forrester report by vp and principal analyst Andras Cser: **"Legacy fraud (fraudsters using stolen credit card numbers to complete unauthorised payments) is still rampant, and as merchants and issuers improve their payment fraud defences, fraudsters are turning toward less detectable fraud patterns, such as policy abuse, return fraud, and hoarding."** According to a Forrester research survey, 58% of the retail market will increase investments in solutions to prevent bot and payment fraud activities combined.

Various banks and telecommunications companies are also attractive targets for external schemes. Telecommunications fraud continues to impact companies globally, with a 12% increase in fraud loss reported in 2023 compared to 2021, equating to an estimated $38.95 billion lost in 2023, representing 2.5% of telecommunications revenues.



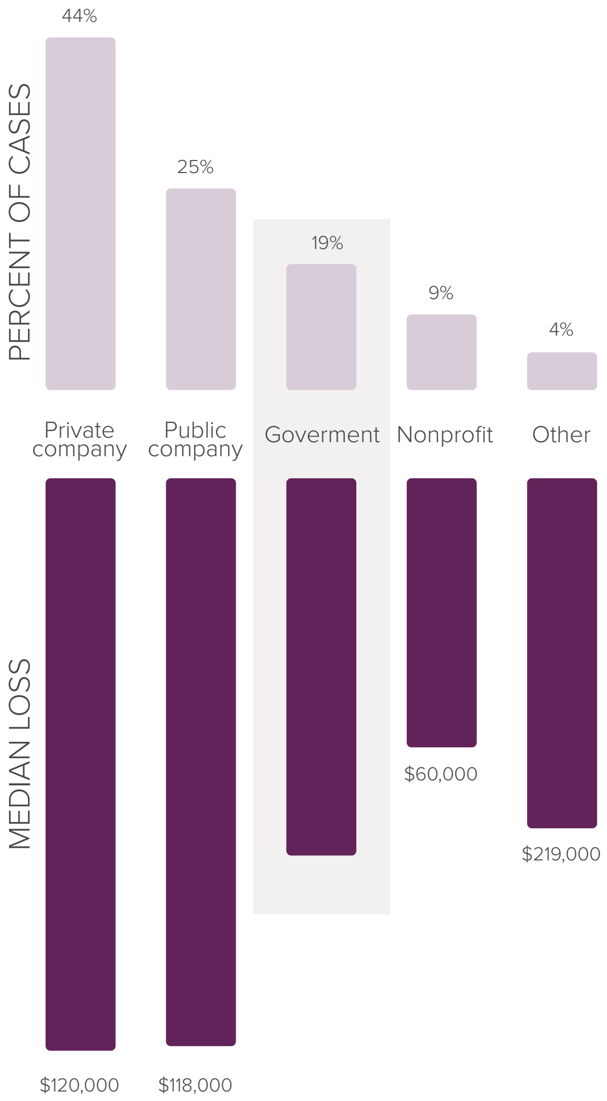
Note: Percentages may not total 100 because of rounding.
Base: 550 business and technology professionals working in retail
Source: Forrester's Priorities Survey, 2023

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Fraud Management Investments In Retail | "What are your organization's investment plans for each of the following retail initiatives over the next 12 months?"

"Today, EFM solutions are real-time data ingestion platforms that must respond to payment fraud management requirements (account-to-account transfers) with instantaneous risk-scoring engines. EFM solutions must be able to intercept fraudulent transactions in real time. Payments are multifaceted and dictate that the EFM solution offers a highly flexible data schema, as well as the ability to participate in data federation with core banking systems across multiple areas (including ATM, ACH/wire, and online bill pay)". Forrester's "The Enterprise Fraud Management Solutions Landscape, Q1 2024", by Andras Cser

With consumers increasingly turning to mobile apps to manage their bank accounts, 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 enable risk departments to analyse multiple pieces of cross-channel data.



ACFE, Occupational Fraud 2022: A Report to the nations

According to the ACFE's 2023 Report to the Nations, a single case of internal fraud cost for organisations reduced from $138,000 to $117,000 in 2023. The types of fraud affecting organisations include public corruption, contract fraud, bribery, beneficiary frauds, and false claims. In 2020, organised crime groups defrauded the French state out of millions of euros meant for workers left jobless by the coronavirus lockdown.

Money mules

An often-underestimated aspect of financial fraud involves the use of money mules and mule accounts. These accounts, frequently established using synthetic identities, play a crucial role in laundering illicit funds. Rapid identification and closure of these mule accounts by financial institutions can disrupt significant portions of the financial crime network. However, pinpointing these accounts has become increasingly intricate, as fraudsters continuously refine their strategies to evade detection. Acting as the vital link in fraudulent activities, money mules facilitate the transfer of stolen funds to criminals.

Merchant fear

When retailers adopt overly cautious approaches, they risk declining good orders as well. A recent study revealed that over half of declined orders are usually authentic and should have resulted in successful conversions. In a striking example, during the 2022 holiday season alone, merchants turned away an estimated $24 billion in legitimate orders due to their fear.

A balancing act

The fear extends beyond merchants. Banks tend to block suspicious transactions too, sometimes turning it into a witch hunt, resulting in the loss of customers. It is indeed difficult and costly to accurately determine whether a transaction is fraudulent, which might result in a gradual client base reduction if done incorrectly. According to a recent survey conducted by Fezerai, 77% of respondents would leave their bank if they do not receive a refund for a scam, while 79% of respondents aged 25 to 44 years would leave the bank if it ever blocked a legitimate transaction, even if the matter is quickly resolved.

A typical fraud case lasts

12 months

before detection

and causes a **median loss** of

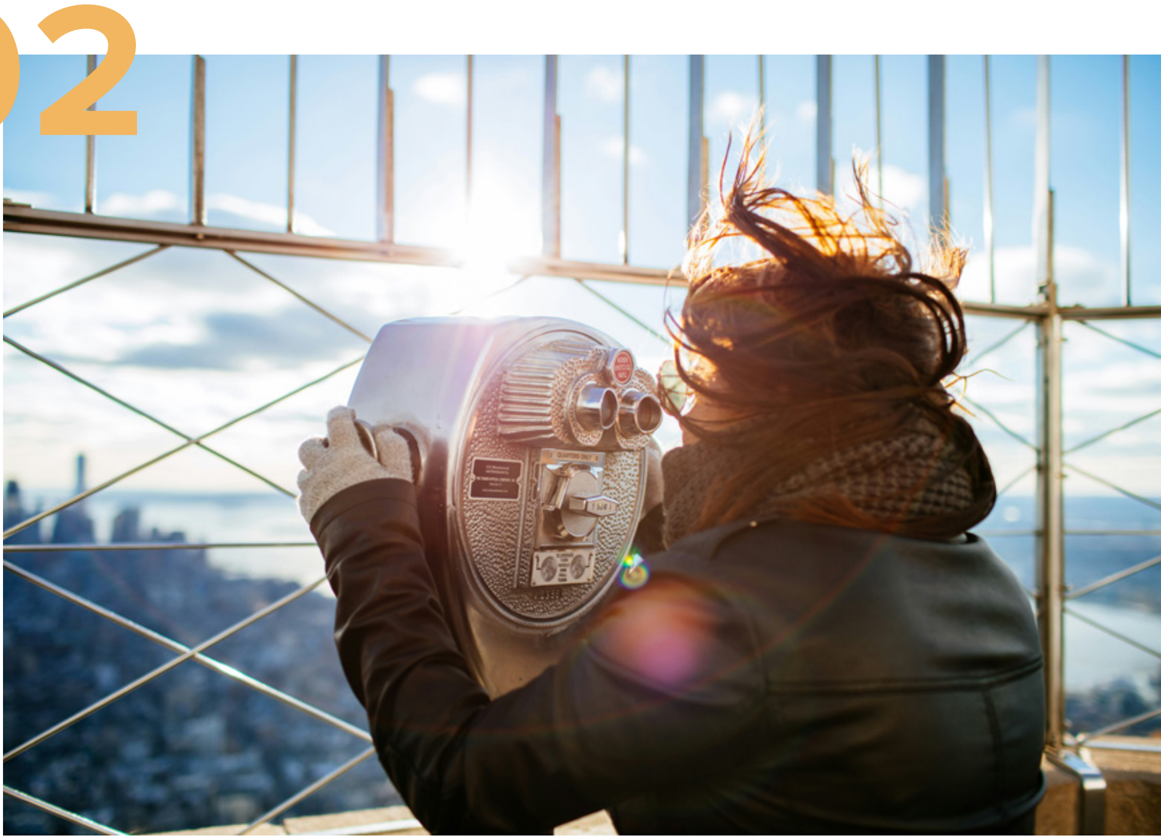
$117,000

Source: Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations

Chapter 02

Fraudsters' Modus Operandi

02



Social engineering fraud and cross-border operations against cyber criminals

Individuals are markedly more susceptible to fraud and hacking than governments or businesses. Social engineering fraud comprises a broad spectrum of deceptive methods used by criminals to exploit people's trust, aiming either to extract money directly or to gather sensitive information for future illicit activities.

Operation First Light, spearheaded by Interpol, targeted 33 call centres across Asia, resulting in the arrest of over 1,000 suspects involved in orchestrating phone scams globally. This operation, initiated in September 2019 and extended into 2021 due to the COVID-19 crisis, unveiled thousands deceived into remitting funds under the guise of aiding relatives in dire emergencies or through impersonation of public officials, culminating in the seizure of assets valued at $3.47 million.

These frauds frequently leverage diverse communication channels, with a particular predilection for social media, though telephone or face-to-face interactions are also common. Social engineering fraud's repertoire includes phishing, vishing, and SMiShing, alongside telecom fraud, business email compromise (BEC), romance scams, investment frauds, voice scams, and the exploitation of remote access tools (RATs). The FBI's 2021 Internet Crime Report highlighted that 323,972 individuals reported falling prey to these fraud types, incurring collective losses nearing $45 million.

Further, an international BEC fraud, implicating a Hungarian company and its Hong Kong associates in a scheme defrauding $8.6 million, was dismantled by a collaborative effort from Interpol, Europol, and the NCB in Budapest. The Interpol Orange Notice has been issued as a caution against the counterfeit, theft, and illicit promotion of fake COVID-19 and flu vaccines. The early months of 2020 saw nearly 1 million COVID-related spam messages and 48,000 malicious URLs. January 2021 marked the takedown of the largest illegal dark web marketplace in a concerted international effort, involving multiple countries, removing a platform that served half a million buyers and 2,400 sellers. These instances underscore the extensive, cross-border nature of modern fraud schemes.

Artificial intelligence

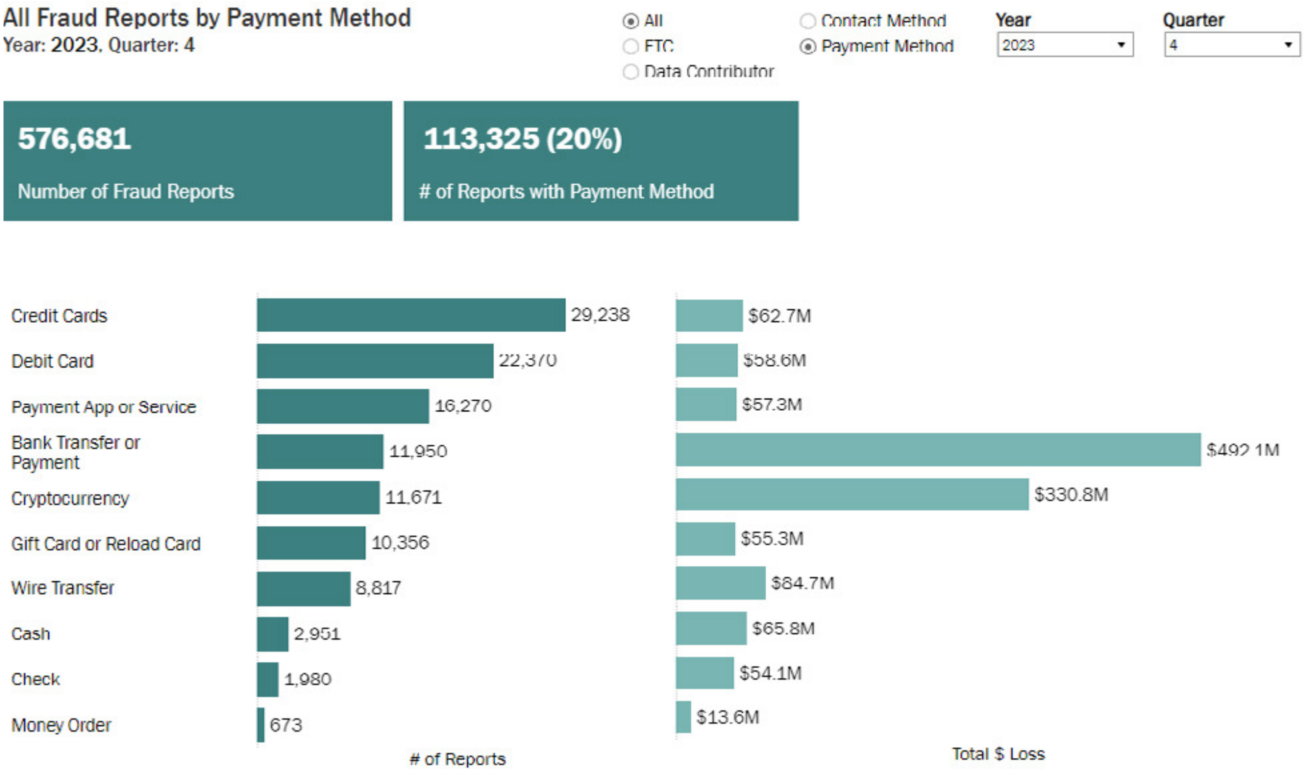
Artificial intelligence, especially Generative AI technologies, has ushered in novel avenues for fraud, notably within the sphere of social engineering. These tools empower criminals to manipulate individuals, craft fictitious personas, and execute scams with unprecedented efficiency and sophistication.

Image generation for persona creation: Generative AI can produce lifelike images, allowing fraudsters to construct believable personas for scams. Through these convincing visuals, perpetrators create false identities to deceive both individuals and organisations.

Deepfake audio and video for impersonation: Utilising Generative AI, deepfake technology synthesises audio and visuals that accurately mimic human voices and appearances. These deepfakes are exploited to impersonate notable figures, such as bank officials or executives, facilitating the authorisation of fraudulent transactions involving substantial sums.

Phishing message production: Fraudsters craft compelling emails, text messages, or social media communications, ensnaring individuals into revealing sensitive information or partaking in deceitful transactions.

The advent of AI tools has significantly lowered the entry threshold for novice hackers. These tools assist in automating the discovery of vulnerabilities and simplifying password cracking. Moreover, in July 2023, the US FBI highlighted concerns over the use of AI by novice hackers to create, modify, and enhance malware—a task traditionally requiring significant technical skill. The modification of malware complicates its detection by antivirus software due to the absence of recognisable patterns or signatures.



All Fraud Reports by Payment Method
Year: 2023, Quarter: 4

● All
○ FTC
○ Data Contributor
○ Contact Method
● Payment Method

Year: 2023
Quarter: 4

576,681
Number of Fraud Reports

113,325 (20%)
# of Reports with Payment Method

Source: Federal Trade Commision, statistics for 2024

The proliferation of AI-generated deepfakes poses an increased risk to the financial sector, opening up new fraud possibilities, some of which have already led to substantial financial losses. For instance, in 2020, the convincing use of deep voice technology misled a Hong Kong bank manager into transferring $35 million to fraudsters, under the belief he was communicating with a familiar company director[4].

Card fraud

In countries where card penetration is high, card fraud remains the most common type of fraud. According to the statistics from Federal Trade Commision for 2024, Credit cards are the highest means of fraud out of all reports (29 238 reports), yet Bank Transfer and Payment has the largest volume, followed by the cryptocurrency. 492M USD and 330M USD respectively.

[4] https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=7b25d8d87559

A 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 unauthorised 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 periodic statements. This allows fraudsters to buy time.

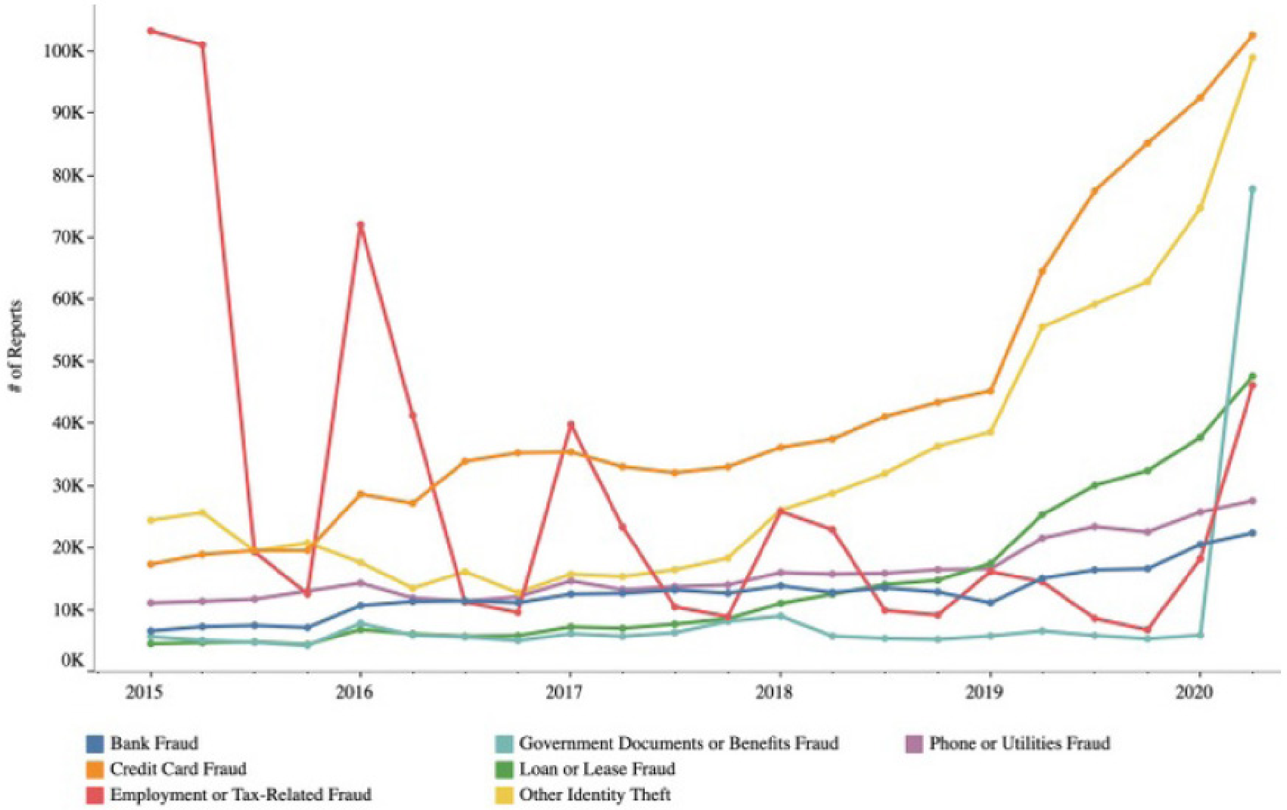
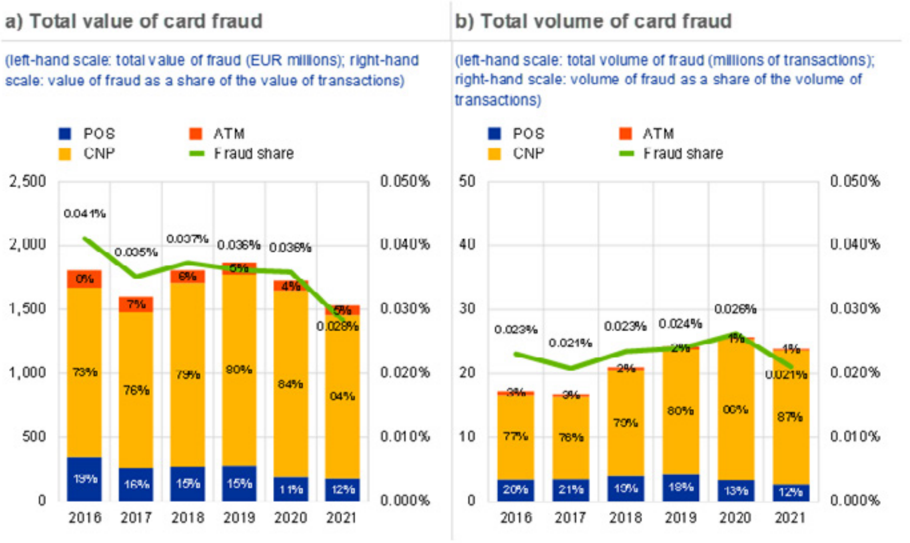


Image credit: Tableau Publuc • Data Source: Federal Trade Commission

Total value and volume of card fraud using cards issued within SEPA



a) Total value of card fraud

(left-hand scale: total value of fraud (EUR millions); right-hand scale: value of fraud as a share of the value of transactions)

b) Total volume of card fraud

(left-hand scale: total volume of fraud (millions of transactions); right-hand scale: volume of fraud as a share of the volume of transactions)

Source: All reporting card payment scheme operators.
Note: POS stands for "point of sale"; CNP stands for "card-not-present".

Value and volume of fraud types as a share of total card fraud using cards issued within SEPA | European Central Bank (2023)

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 accelerated the adoption of e-commerce, which boosted the rise in CNP payments; golden opportunities for fraudsters.

In previous years, the vast majority of card fraud related to CNP transactions[5]. In both 2020 and 2021, CNP fraud accounted for approximately 84% of the total value of card fraud. This share had been growing steadily, in line with the continuously increasing importance of e-commerce and the use of card payments over the internet. Despite it, ECB found that in 2021 the total value of CNP fraud amounted to €1.28 billion, showing a strong decline compared with 2020 (-12.1%). The majority of CNP fraud continued to take place across borders.

This trend is reflected in European fraud statistics that were issued by the European Central Bank in the ECB's yearly report. According to Insider Intelligence the CNP fraud loss is projected to reach 13bln USD by the end of 2024 in just US only, for all world combined the numbers can easily triple.

[5] ECB 2023

Transaction laundering

Transaction laundering represents a sophisticated fraud mechanism that demands vigilance. It occurs when a merchant processes payments for another merchant's website clandestinely, without the acquiring bank's knowledge. This often pertains to transactions involving prohibited goods or services. The complicit merchant, serving as a 'mule,' profits from facilitating these transactions.

Payment Service Providers (PSPs) and acquirers face the risk of reputational harm and significant penalties from card associations due to transaction laundering. Instances have been noted where merchants unknowingly became conduits for transaction launderers. Upon discovery, backed by solid evidence from card associations, these merchants struggle to establish their innocence. The scrutiny around this fraud type by card organisations intensifies, given its exploitation of the flourishing e-commerce sector.

Friendly fraud

Friendly fraud, also known as chargeback fraud, poses a significant challenge to e-commerce, identified by the FBI as one of the top three challenges facing online businesses. Despite the benign implication of its name, friendly fraud is a major source of chargeback fraud, inflicting substantial financial damage on online retailers without necessarily involving organised criminal activities. Merchants are expected to face over $100 billion in chargeback losses this year alone, with friendly fraud estimated to constitute an astonishing 61% of all chargebacks.

This form of fraud takes place when consumers dispute online purchase transactions with their banks, leading to chargebacks. The financial impact of friendly fraud falls heavily on merchants, who end up bearing over 75% of the associated costs, significantly exacerbating losses from fraudulent chargebacks. With global e-commerce fraud losses projected to surpass $343 billion in online payments by 2027[6], the challenge of friendly fraud is not to be underestimated, even though it may not always stem from sophisticated criminal endeavours. Its effect on the financial wellbeing of businesses is profound and wide-reaching.

Authorised Push Payment (APP) Fraud

Authorised Push Payment (APP) fraud involves fraudsters using phishing tactics to trick customers into authorising real-time transfers to accounts they control. These fraudsters often pose as legitimate businesses or service providers, claiming payment for alleged services. Unwitting customers authorise these payments, leading to direct fund transfers to the fraudster's account. APP fraud has become increasingly prevalent, now representing the largest fraud category in the UK and posing significant challenges worldwide.

In 2023, an astonishing 77% of APP fraud incidents, accumulating over £239 million[7], were

[6] https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/

[7] https://www.ukfinance.org.uk/news-and-insight/press-release/criminals-steal-over-half-billion-pounds-and-nearly-80-cent-app

conducted online. These schemes typically convince individuals or businesses to send money to fraudster-controlled accounts under the guise of legitimate transactions. The complexity of these frauds, amplified by the use of Generative AI technologies, presents a major hurdle for the financial sector. It highlights an urgent need for improved security protocols and increased awareness among consumers to combat the growing threat of APP fraud effectively.

Application fraud

Application fraud occurs when individuals use their own identity or fabricated identities to apply for loans or credit cards. Known as first-party application fraud, this type of deceit involves the fraudster receiving approval for financial products, withdrawing the funds, and then vanishing. A significant portion of this fraud, approximately 40%, involves the creation of synthetic identities. These are constructed by amalgamating data from various sources, often stolen, to create a new, fictitious identity. This method is particularly challenging to detect as it blends genuine information with fabricated details, making the synthetic identities appear credible during the verification process.

Counterfeit fraud

Counterfeit fraud involves the illegal duplication of legitimate card data onto fraudulent cards. This type of fraud often employs devices known as skimmers, which are illicitly installed in locations such as gas stations, restaurants, movie theatres, or ATM machines to capture card information. To capture PIN codes, criminals may also use hidden micro-cameras. Detecting skimming devices is challenging. The widespread adoption of EMV chip technology in regions where it has been extensively implemented has led to a significant decrease in counterfeit fraud, with a reduction of 75% reported by VISA in 2019.

Additionally, phishing, smishing (SMS phishing), and vishing (voice phishing) are techniques used by fraudsters to “fish” for personal and financial information via email, SMS, or voice messages, respectively. A notable variation of these schemes is the romance scam, where fraudsters exploit social media and dating applications to build an emotional connection with their victims, eventually convincing them to financially assist the fraudster with fabricated emergencies or problems.

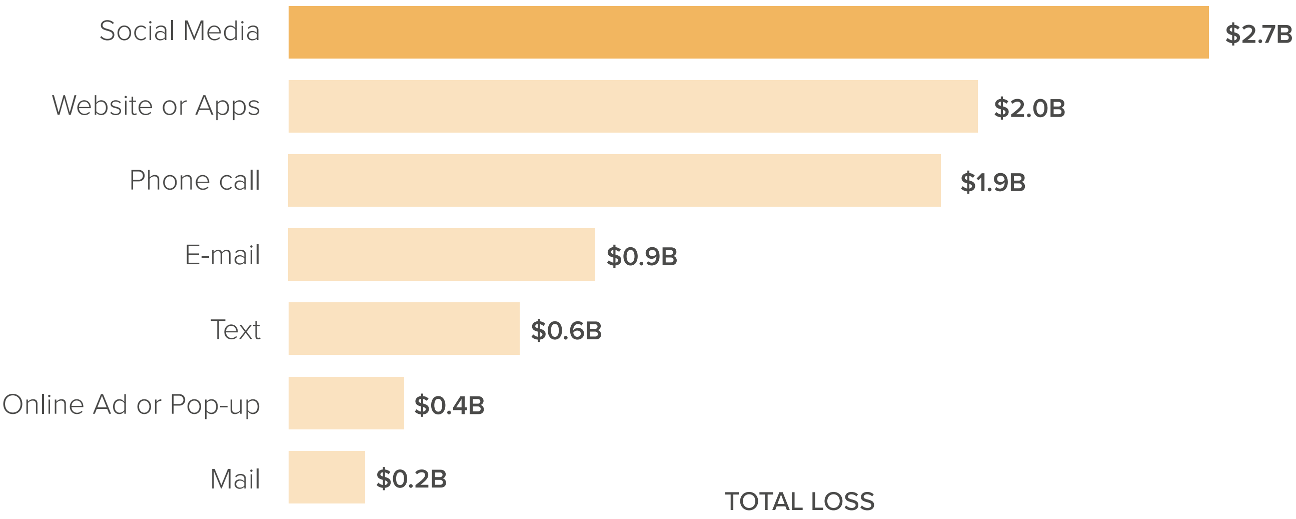
Social media fraud

Social media has evolved into a primary interface for Generation Z and millennials, transforming from mere communication platforms to comprehensive e-commerce ecosystems. The incidence of social media fraud scams saw a threefold surge in 2019, a trend that notably intensified following the global lockdowns. The U.S. Federal Trade Commission (FTC) identifies social media as a significant enabler for scammers, underlining its critical role in perpetuating fraudulent schemes. The FTC reports that since 2021, one in four individuals who filed reports of financial loss due to fraud pointed to social media as the origin of their scam encounter. Between January 2021 and June 2023, the financial damages reported from these scams reached an astonishing total of $2.7 billion, highlighting the pressing challenge social media fraud presents in the digital age.

Reported fraud losses by contact method

January 2021 - June 2023

More money was reported lost to fraud originating on social media than by any other method of contact.

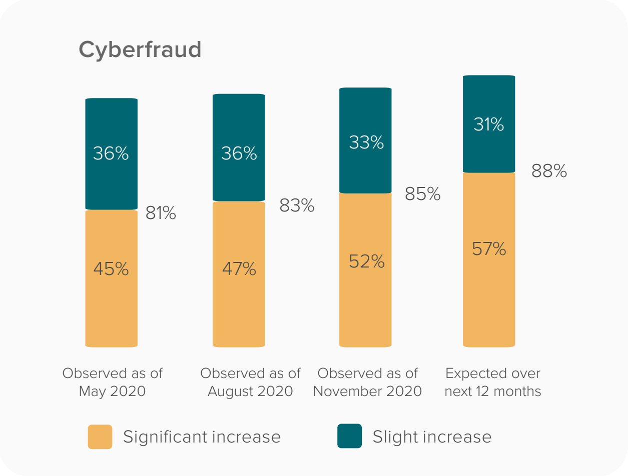


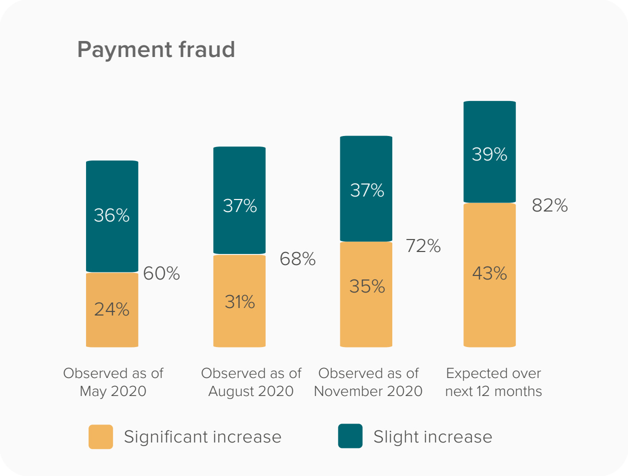
Not shown are contact methods classified as other, including TV or radio, print, fax, in person, and other methods consumers write in or that cannot be otherwise categorized.

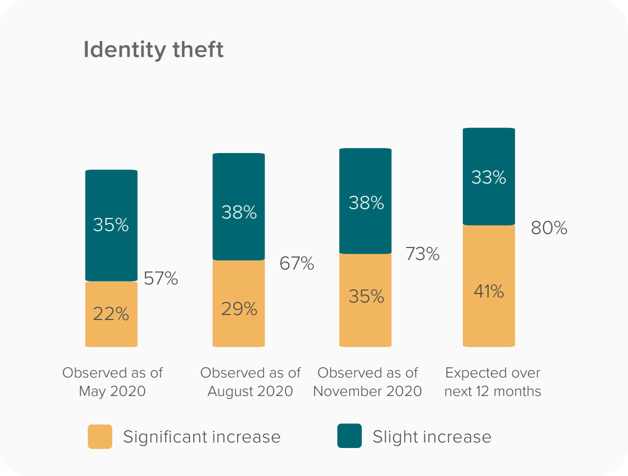
Reported scams frequently involve online shopping, romance deceptions, and counterfeit income opportunities. A significant number of complaints concern online retailers failing to fulfil product deliveries, with nearly a quarter of victims enticed into purchasing products or services through misleading advertisements. Lost and stolen card fraud, along with Card-Never-Arrived fraud, manifest when debit or credit cards are either misplaced or unlawfully taken and subsequently exploited by criminals, or when a newly issued card is intercepted by fraudsters before reaching the legitimate cardholder.

Identity Theft

Identity theft, also known as ID theft, occurs when cybercriminals utilise stolen credit cards or their numbers to conduct unauthorised purchases. The Operation Carding Action 2020 notably disrupted the illicit trade of stolen credit card data on the dark web, involving law enforcement collaboration from Italy, Hungary, and the UK. Interpol's analysis of 90,000 pieces of credit card data averted approximately US$48 million in potential losses to consumers and financial institutions. Traditionally, the elderly were frequent targets, yet recent trends indicate a shift, with a significant uptick in



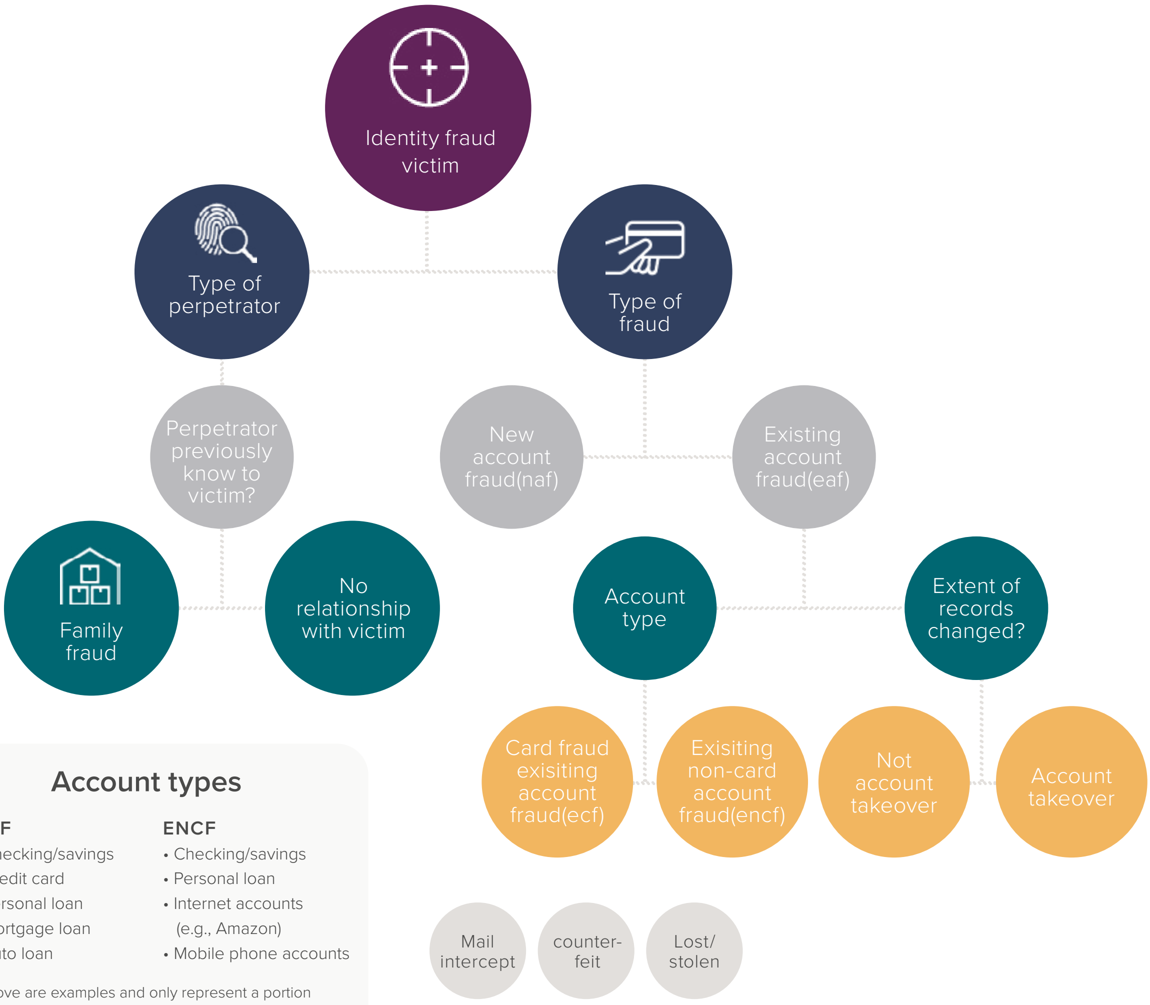




victims aged between 41-50 years old—showing a 43% increase for this demographic. This pattern mirrors findings in the US, where the Federal Trade Commission processed 1.1 million fraud reports in 2022, with 15% attributed to individuals aged 20-29 and 16% to those over 70 years old. Similarly, in Canada, Equifax reported millennials as increasingly becoming primary targets for fraudsters.

A recent study highlighted in Payments Cards and Mobile (November 2023) reports a significant 17% rise in synthetic fraud cases over the last two years, as observed from a survey of 500 fraud and risk professionals across the financial services and fintech sectors in the United States. The study reveals that over one-third of these professionals have witnessed a substantial increase of 20-50% in such incidents. Synthetic identity fraud, which intricately combines authentic personal information with fabricated details to construct convincing false identities, has become increasingly complex and difficult to detect, largely due to advancements in AI technology. This emerging challenge

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


Identity fraud victim
Type of perpetrator
Type of fraud
Perpetrator previously know to victim?
New account fraud(naf)
Existing account fraud(eaf)
Family fraud
No relationship with victim
Account type
Extent of records changed?
Card fraud exisiting account fraud(ecf)
Exisiting non-card account fraud(encf)
Not account takeover
Account takeover
Mail intercept
counter-feit
Lost/ stolen

Account types

NAF

- Checking/savings
- Credit card
- Personal loan
- Mortgage loan
- Auto loan

ENCF

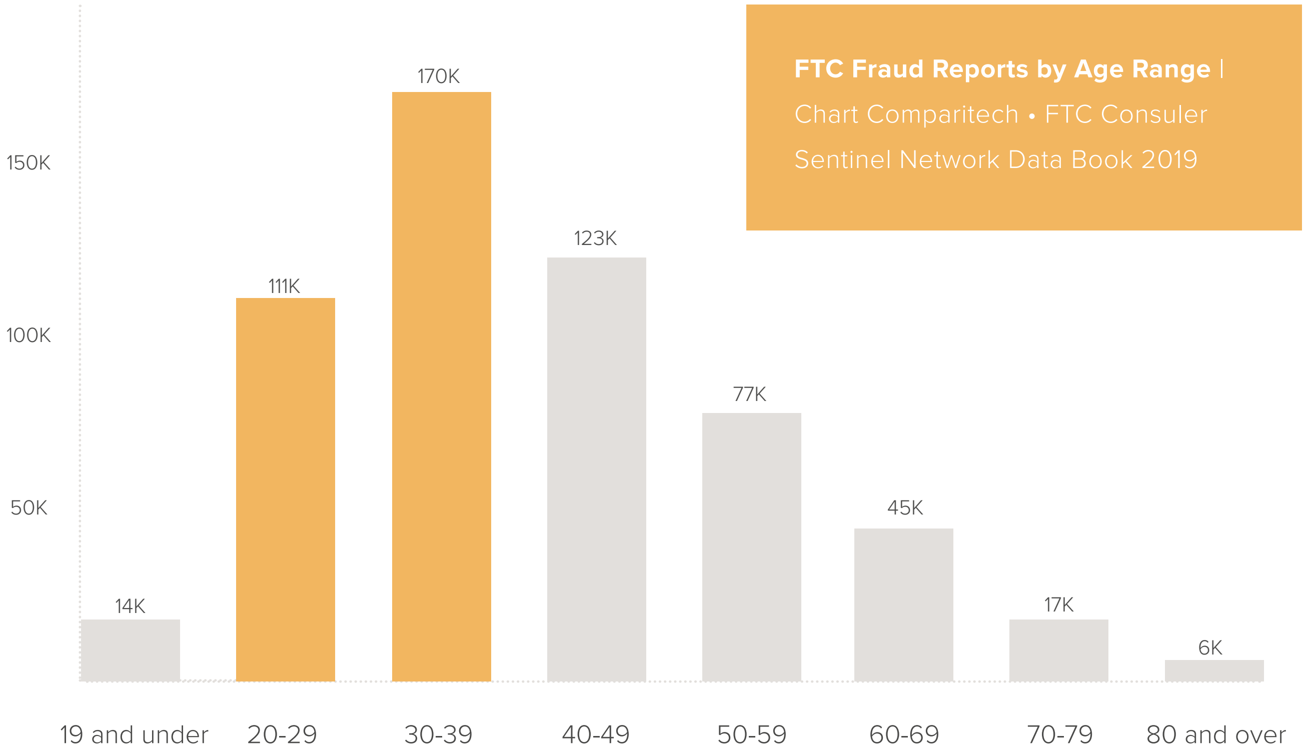
- Checking/savings
- Personal loan
- Internet accounts (e.g., Amazon)
- Mobile phone accounts

*Above are examples and only represent a portion of the accounts in each category.

underscores the urgent need for enhanced detection and prevention strategies in combating this sophisticated form of fraud.

This connection brings us back to the discussion on Generative AI. The advent and improvement of such technologies have provided fraudsters with powerful tools to swiftly generate synthetic identities. These fabricated personas are sophisticated enough to bypass conventional fraud prevention mechanisms, such as document verification and manual checks. This rapid evolution represents a significant challenge for the financial sector. Experts are increasingly recognizing that fraudsters’ capabilities are advancing more quickly than the development of countermeasures. This dynamic underscores the critical need for the financial industry to innovate and adapt its defensive strategies to keep pace with these evolving threats.

Identity theft, best illustrated through this accompanying diagram, involves unauthorised transactions leading to chargebacks against



FTC Fraud Reports by Age Range | Chart Comparitech • FTC Consuler Sentinel Network Data Book 2019

merchants, thereby affecting both cardholders and businesses.

Cifas, the entity managing the UK's most extensive fraud prevention database, disclosed that identity fraud cases hit a record peak in 2022. Out of 409,000 reported instances, identity fraud constituted 68% of the total entries in the British National Fraud Database, marking a 23% increase from previous figures. This surge highlights the growing challenge of identity theft, affecting a broad spectrum of stakeholders within the financial ecosystem.

Contrary to previous patterns where the elderly were the primary targets, recent trends show a significant number of victims falling within the 30-39 age bracket. This shift is evident in the United States, where the Federal Trade Commission (FTC) processed 1.6 million fraud reports in 2019, with a notable 33% originating from individuals aged 20-29, and only 13% from those over 70. Equifax in Canada mirrors this trend, indicating that millennials have increasingly become prime targets for fraud. This demographic shift underscores the need for heightened awareness and preventive measures among younger populations, who are now more likely to be exploited by fraudsters.

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

Account takeover

Account takeover involves unauthorised control over another individual's genuine card account, often leveraging personal information obtained via data breaches. This type of fraud allows criminals to impersonate the legitimate cardholder and falsely report theft or loss to request a replacement card. Without vigilant transaction history monitoring by cardholders, such takeovers may go undetected for extended periods. Recently, account takeover incidents have surged by 57%, with Javelin Strategy reporting that 40% of these takeovers occur within 24 hours after a fraudster accesses a victim's account.

The escalation of account takeover fraud is partly attributed to inadequate password management practices[8]. A considerable portion of the population uses weak, reused, or easily guessable passwords, significantly facilitating fraudulent access to multiple accounts. In 2022, the Federal Trade Commission (FTC) received over 725,000 reports of impostor scams, reflecting a slight decrease from nearly a million reports in 2021 but marking the highest financial loss recorded since 2018, with consumers losing $2.67 million.

UK Finance documented 34,114 instances of card identity theft in just the first half of 2022, leading to a gross loss of £21.4 million[9]. These scams, often a combination of account takeover and identity theft, illustrate a sophisticated fraud strategy where criminals create new accounts or gain control over existing ones, representing 35.62% of the total 5.2 million fraud reports filed with the FTC in 2022.

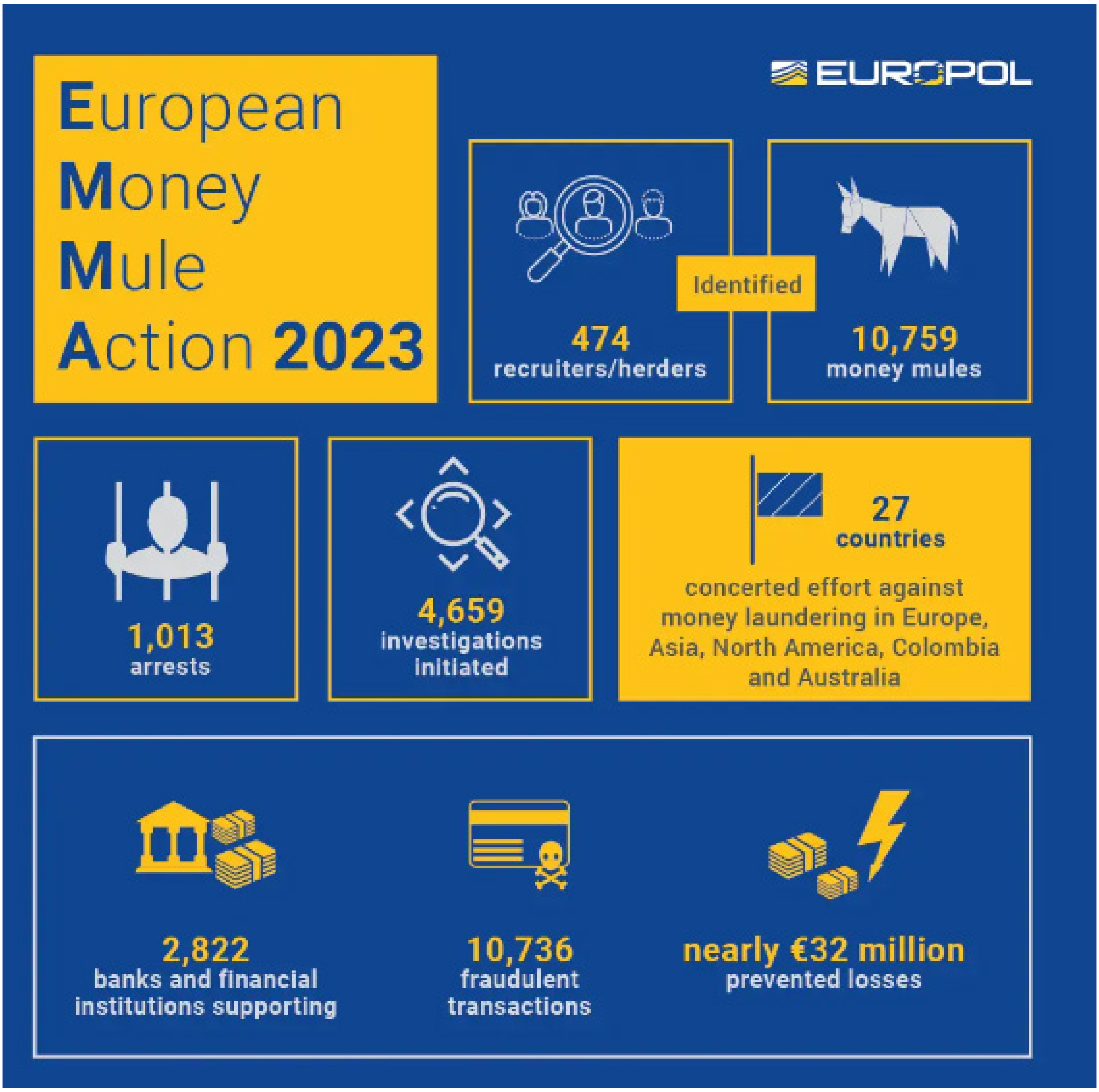
Mule Accounts

Money mules play a crucial role in financial fraud, often by creating or hijacking bank accounts to launder proceeds from criminal activities. Remarkably, over 59% of new account fraud is attributed to money mules. These individuals facilitate the evasion of bank scrutiny, significantly complicating the process of tracing funds acquired through scams or account takeovers. In 2023, Europol and the European Money Mule Action (EMMA) identified over 10,000 money mules, leading to more than 1,000 arrests and the prevention of approximately 32 million EUR in potential losses.

Despite their seemingly minor role, money mules are a critical component of the fraud ecosystem. Their activities enable broader financial crimes by providing a mechanism to launder illicit funds, making it imperative for financial institutions to detect and disrupt these operations. By focusing on intercepting money mule activities, banks can address financial crime more effectively at its source, safeguarding their operations and protecting their customers from fraud.

[8] Sift' "Q3 2023 DIGITAL TRUST & SAFETY INDEX" report

[9] https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf



EUROPOL

European Money Mule Action 2023

Identified

474 recruiters/herders

10,759 money mules

1,013 arrests

4,659 investigations initiated

27 countries

concerted effort against money laundering in Europe, Asia, North America, Colombia and Australia

2,822 banks and financial institutions supporting

10,736 fraudulent transactions

nearly €32 million prevented losses

Source: Europol

Chapter 03

Who is the fraudster?

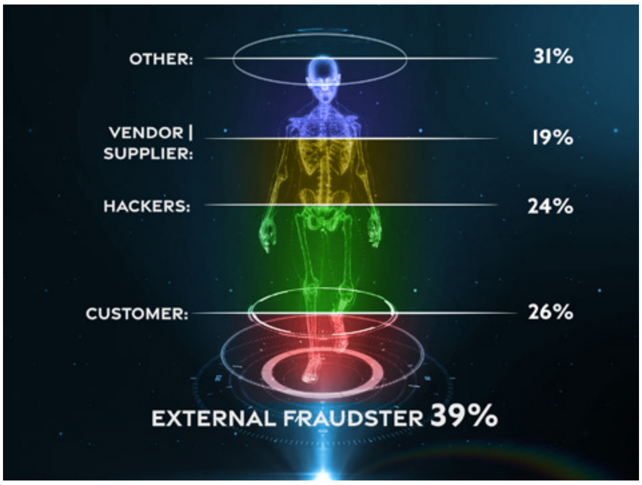
03

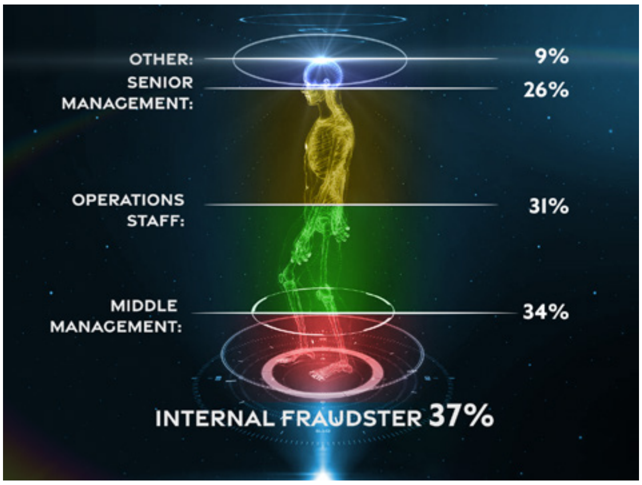
The identity of the fraudster is evolving, encompassing individuals who operate from within an organisation, externally, or through collusion between the two. PWC[10] reports highlight a growing trend of fraud committed by the internal management class or through collusion between internal and external fraudsters. This introduction paves the way for a detailed examination of the fraudster's nature, reflecting the diverse and changing landscape of fraud perpetration.

The external fraudster

External fraudsters, comprising hackers, customers, vendors, and suppliers, account for three-quarters of all external fraud activities. Fraudulent customers may engage in issuing bad cheques or submitting

[10] Global Economic Crime and Fraud Survey" of 2020, PwC



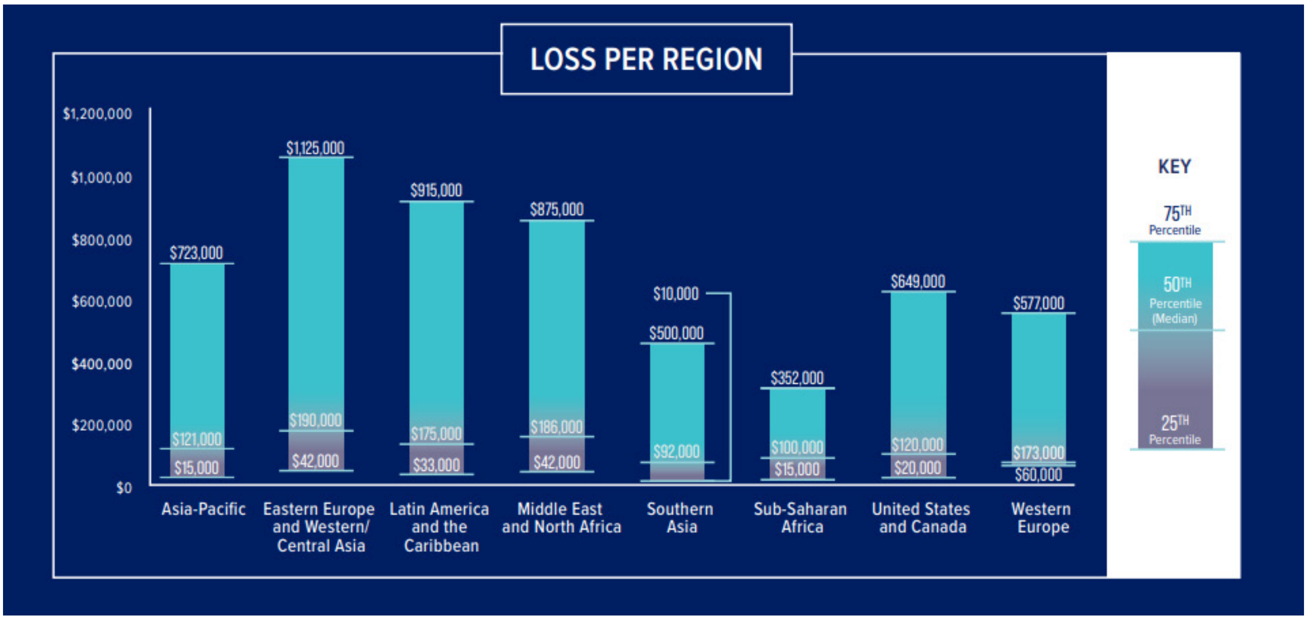


falsified account details for payments, as well as attempting returns of stolen or counterfeit products for refunds. Dishonest vendors and suppliers might partake in bid-rigging, invoice for undelivered goods or services, or solicit bribes from company employees. Moreover, organisations encounter security breaches and intellectual property theft conducted by unidentified third parties. Other manifestations of external fraud include hacking, proprietary information theft, tax evasion, bankruptcy fraud, insurance deceit, healthcare scamming, and loan fraud, showcasing the broad spectrum of threats posed by external actors in the fraud landscape.

The pandemic has significantly boosted online sales, compelling companies involved in e-commerce to seize the momentum. This surge in demand often leads to supply chain challenges, pushing businesses to engage with alternative suppliers and delivery services. In the rush to accommodate increased demand, businesses might bypass essential due diligence processes designed to mitigate fraud risk. This lapse exposes them to potential dealings with fraudulent or inexperienced suppliers, or even collusion among employees and third-party entities. Furthermore, the pandemic has intensified the number of business transactions between companies and governments, with firms vying for lucrative government contracts. This scenario is ripe for corruption, particularly in regions where such practices are prevalent, thereby escalating the risk of bribery. This complex situation underscores the importance of stringent due diligence and anti-fraud measures to safeguard businesses in these challenging times.

The internal fraudster

Internal fraudsters, also known as occupational fraudsters, pose a significant threat to businesses and organisations. A comprehensive survey by the Association of Certified Fraud Examiners (ACFE)



reveals that 65% of internal fraud perpetrators are company employees, with 38% having been with the company for over six years. These individuals are responsible for double the average fraud losses, amounting to approximately $200,000. Alarmingly, 20% of these fraudsters occupy executive or C-level positions, inflicting the most substantial average fraud losses of around $600,000. Their positions of authority and the trust they have cultivated within the company allow them to bypass internal controls with relative ease. Although fraud loss figures vary by region, the global estimate suggests that the total impact runs into the trillions, highlighting the pervasive and profound economic effects of internal fraud across industries worldwide.

Collusion

Collusion in fraud involves a collaboration that crosses the internal-external divide, with about 20% of all fraud schemes resulting from such partnerships. These collusive efforts typically include a mix of individuals from both inside and outside the targeted company. When successful and undetected, these groups are likely to replicate their fraudulent activities, securing substantial illicit gains. The collusion frequently involves a network of accomplices, such as former employees, vendors, suppliers, or customers, who coordinate their actions with a corrupt insider. This phenomenon underscores the critical necessity for enhanced due diligence procedures with third parties, aiming to identify and mitigate these complex threats to organisational integrity and financial security.

2,110 cases from **133** countries

Causing total losses of more than **$3.6 billion**

$1,783,000 average loss per case

21% of cases had losses of $1 million+

CFEs estimate that organizations **lose**

5% of revenue to **fraud** each year

Projected against 2021 GWP **($94.94 trillion)**

that's more than **$4.7 trillion** lost to **fraud globally**

Source: Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations

Asset misappropriation schemes
are the most common but least costly

86% off cases

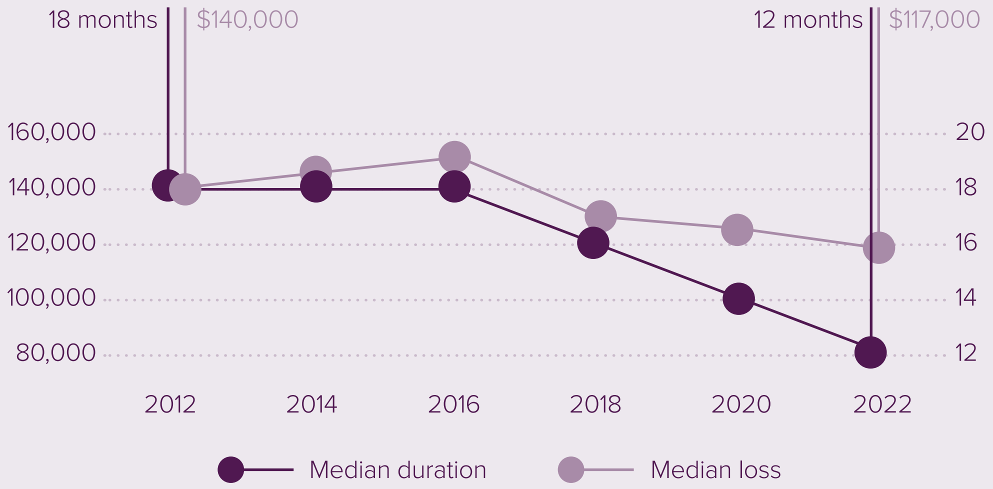
$100,000
median loss

Financial statement fraud schemes
are the least common but most costly

9% off cases

$593,000
median loss

A decade of occupational fraud: trends from 2012-2022

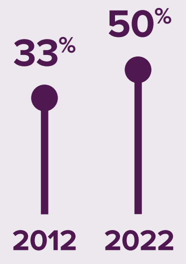


Frauds are being caught **faster** and causing **smaller** losses.

Median losses down
⇩ 16%

Median duration down
⇩ 33%

The percentage of cases involving **corruption** is on the **rise**



Fraudsters
are **collaborating more**

1 Perpetrator

58% 2012 ⇩ **42%** 2022

2+ Perpetrator

42% 2012 ⇧ **58%** 2022

Source: Association of Certified Fraud Examiners, Occupational Fraud 2022: A Report to the Nations

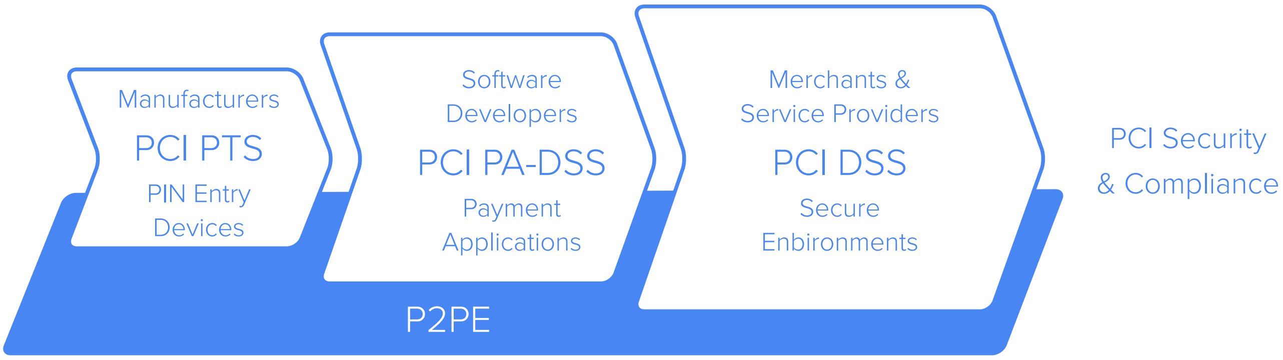
Chapter 04

Security, Detection and Prevention

04

Payment card industry security standards

Protection of Cardholder Payment Data

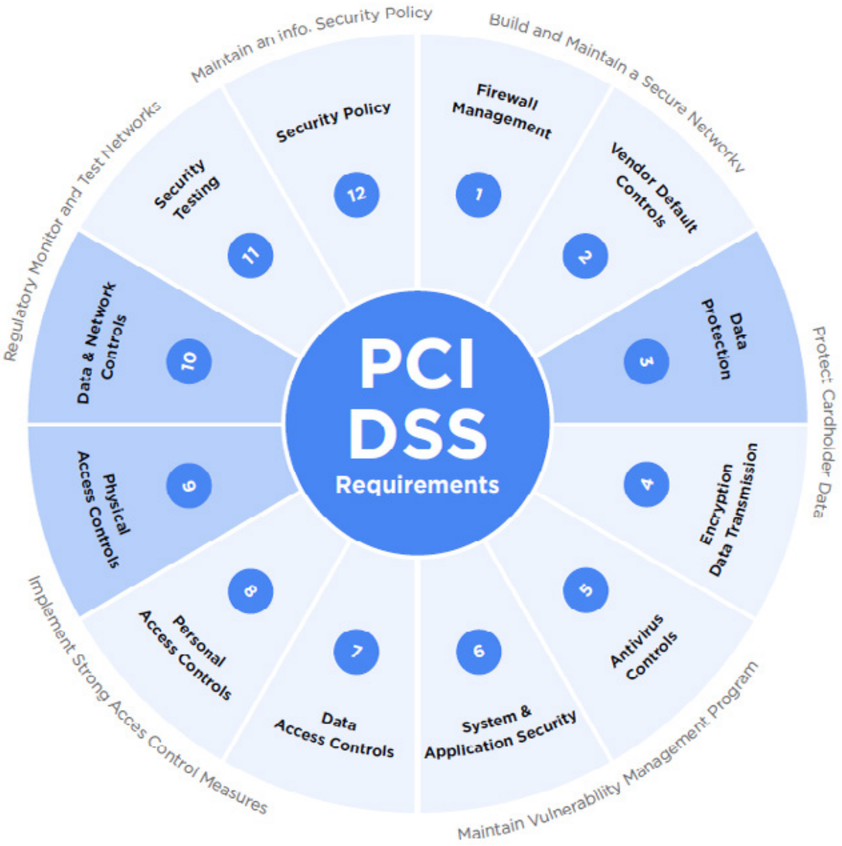


Ecosystem of payment devices, applications, infrastructure and users

Source: PCI Security Standards Council

Legal Compliance

Financial institutions entrusted with processing payment transactions are required to adhere to the Payment Card Industry Data Security Standard (PCI DSS), a comprehensive set of industry regulations established by the PCI Security Standards Council. Founded in 2006 by five major card schemes—VISA, MasterCard, JCB International, American Express, and Discover—the Council's primary objective is to furnish the global payments industry with regularly updated legal security standards. Through its initiatives, the PCI Security Standards Council assists merchants and financial institutions in comprehending and implementing protocols for security policies, technologies, and ongoing procedures aimed at safeguarding their payment systems from breaches and the theft of cardholder data.


PCI DSS Requirements
Maintain an info. Security Policy
Build and Maintain a Secure Networkv
Protect Cardholder Data
Maintain Vulnerability Management Program
Implement Strong Acces Control Measures
Regulatory Monitor and Test Networks
1 Firewall Management
2 Vendor Default Controls
3 Data Protection
4 Encryption Data Transmission
5 Antivirus Controls
6 System & Application Security
7 Data Access Controls
8 Personal Access Controls
9 Physical Access Controls
10 Data & Network Controls
11 Security Testing
12 Security Policy

PCI-DSS standards

Payment processors are mandated to adhere to basic PCI-DSS standards:

- Installing and maintaining a firewall configuration to safeguard cardholder data.
- Avoiding the use of vendor-supplied defaults for system passwords and other security parameters.
- Protecting stored cardholder data through encryption.
- Encrypting the transmission of cardholder data across open, public networks.
- Utilising and regularly updating anti-virus software or programs.
- Developing and maintaining secure systems and applications.
- Restricting access to cardholder data by business need-to-know.
- Assigning a unique ID to each individual with computer access.
- Restricting physical access to cardholder data.
- Tracking and monitoring all access to network resources and cardholder data.
- Regularly testing security systems and processes.
- Maintaining a policy that addresses information security for employees and contractors.

Payment service providers and merchant acquirers are required to allow periodic regulatory compliance audits. The Wirecard scandal has shaken up the e-payment industry, emphasising the critical importance of thorough audits. Auditors had issued two qualified opinions on the company’s audited financial statements, raising red flags that were largely overlooked.

Risk management

Risk management involves addressing various categories of risk, each requiring specific detection and prevention strategies. Risk professionals must be adept at identifying and mitigating:

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

Fraudsters often camouflage themselves behind legitimate-looking online storefronts, selling illegal products and services while maintaining a facade of legitimacy. Transaction and money launderers exploit web shops as a quick means to launder criminal proceeds. As financial criminals continually evolve their tactics, risk departments must diligently verify the authenticity of merchants' businesses, their ultimate beneficiary owners, historical data, business models, and marketing strategies to identify and investigate suspicious activities.

Payment service providers (PSPs) and acquirers deploy risk management solutions, but the increasing complexity of managing risk across multiple channels and jurisdictions prompts them to seek partnerships with specialised companies in multichannel risk management, compliance, and fraud prevention. These companies leverage cutting-edge technology to provide robust solutions.

According to PwC's 2020 Global Economic Crime and Fraud Survey, organisations with dedicated fraud prevention programs incur lower response and remediation costs compared to those without integrated risk management programs.

The investigation

The investigation process begins with the identification and classification of all relevant risk indicators, including primary and secondary risks. Missing critical indicators could lead to inaccurate risk assessments. Fraud risk, while significant, is just one of several risk categories defined by card associations. The investigation typically follows four key steps:

Step 1: In-depth understanding of the business: Investigators must gain a comprehensive understanding of the business, including assessing the risk level associated with the products or services offered. This involves evaluating the company structure, key markets, geographical locations, and the presence of legally required information on its website and corporate documentation. Identifying the ultimate beneficiary owner (UBO) and C-Level executives is crucial.

Step 2: Data collection: All necessary data must be collected from various sources. This process can be labour-intensive, particularly for web merchants operating across multiple countries and websites. Comprehensive investigation strategies for card-not-present (CNP) merchant acceptance are detailed in resources such as those provided by Webshield Ltd.

Step 3: Data analysis: Once all relevant data is gathered, it must be thoroughly analysed. Innovative link analysis solutions are employed to uncover hidden connections between legal entities, addresses, business relationships, and potential red flags or hits on sanctions lists. AI and ML algorithms help identify hidden patterns indicative of suspicious activity, including analysing digital footprints, social media content, and IP localization, especially in a multi-channel payment environment.

Step 4: Transaction monitoring: Transactions and events from multiple channels are analysed and monitored to detect unusual patterns. Machine learning is instrumental in building risk and fraud models based on known cases, segmenting customers based on KYC and transaction activity, predicting and scoring online transaction risks, and supporting operators in their daily routines, particularly during decision-making and risk assessment phases.

Machine Learning helps:

- To build risk and fraud models based on known cases.
- Segment customers by detecting KYC and transaction activity.
- Predict and score online transactions.
- Assist operators in their daily routines, especially during decision-making and risk assessment phases.

Risk assessment

Risk assessments have undergone a transformation in recent years, moving from manual processes to automated tools that leverage new technologies. Artificial intelligence, particularly rules engines empowered by AI, has revolutionised the way risk professionals gather and analyse data. These tools enable the automatic screening of legal entities against sanction lists, streamlining the process and reducing the potential for false positives. Additionally, machine learning algorithms play a crucial role in enhancing risk assessments by continuously improving their accuracy and efficiency.

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 negatives 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) in 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 customised 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 visualise 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.

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

Compliance with sanction lists is a critical aspect of risk management for all card associations' licensed principal members. These members are required to adhere to regulations set forth by entities like the Office of Foreign Assets Control (OFAC) and local sanction authorities. As part of customer acceptance and identification processes, merchants, their associated directors, and ultimate beneficial owners (UBOs) must undergo screening against sanction lists, including OFAC and Politically Exposed People (PEP) lists.

This screening process, known as enhanced or ongoing due diligence (ODD), is essential for detecting potential instances of fraud, money laundering, transaction laundering, or terrorist financing schemes. By thoroughly vetting individuals involved in the business, especially those at the C-level who oversee operations, financial institutions can mitigate the risk of engaging with entities involved in illicit activities.

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.

Indeed, as highlighted in the preceding chapters, fraud detection and prevention present significant challenges for all stakeholders in the e-commerce and payments industry. Given the complexity of fraud prevention, organisations must allocate resources to dedicated departments equipped with both human expertise and advanced software solutions to effectively mitigate risks over the long term.

While partnering with a company that offers cutting-edge risk solutions may entail initial costs, it represents a prudent investment in safeguarding the organisation against financial and reputational damage in the long run. By leveraging state-of-the-art technology and expertise provided by such partners, businesses can streamline their fraud prevention efforts, ultimately reducing expenses associated with training programs and human resources required to combat fraud independently.

Chapter 05

Conclusion

05

In conclusion, fraud prevention remains a formidable challenge for all participants in the thriving e-commerce and payments sectors. Fraudsters continually target individual consumers, private companies, NGOs, and government institutions, inflicting significant financial and reputational harm. The shift towards online transactions, accelerated by the pandemic, has opened new avenues for fraudsters, with digitally active millennials becoming increasingly vulnerable to social engineering scams.

While traditional forms of fraud such as card fraud and identity theft persist, the emergence of new fraud types facilitated by advancements in Generative AI (GenAI) technology presents a growing threat. E-commerce platforms, now integral to daily life, are experiencing unprecedented exposure to fraud, with projected losses expected to surpass $343 billion by 2027. Social media platforms, evolving into e-commerce hubs themselves, have become significant vectors for fraud, resulting in substantial financial losses for victims.

As the volume and complexity of fraud continue to escalate, stakeholders must remain vigilant and adapt their fraud prevention strategies accordingly. Investing in advanced technologies, robust risk management solutions, and ongoing training programs is imperative to mitigate the risks posed by fraud effectively. By staying ahead of emerging threats and collaborating with trusted partners in the industry, organisations can safeguard their operations and protect against the detrimental effects of fraud on their bottom line and reputation.

Who are these fraudsters?

Fraudsters come from various backgrounds and can be categorised into external and internal perpetrators. External fraudsters operate outside the defrauded company, often with the help of accomplices within the organisation, while internal fraudsters carry out their schemes from within. Customer and business identification and authentication programs, such as Know Your Customer (KYC) and Know Your Business (KYB) procedures, play a crucial role in preventing financial crimes by conducting thorough due diligence on new and existing business relationships.

Advanced technologies like artificial intelligence (AI) and machine learning (ML) are instrumental in detecting suspicious activity by uncovering hidden patterns and analysing transactions and events extracted from multiple channels. These technologies enhance speed, output, and scalability, while link analysis helps connect disparate pieces of information that may be overlooked through manual analysis.

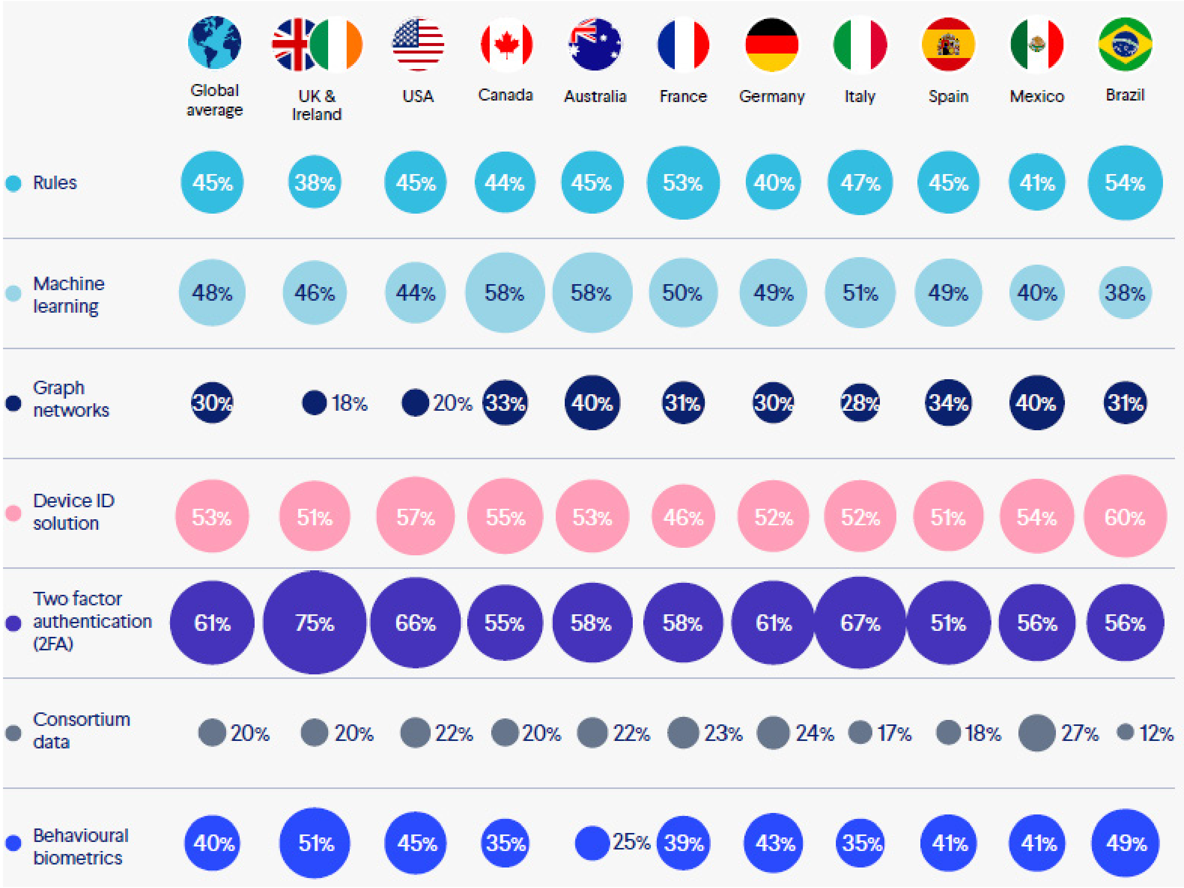
Additional tools like device fingerprinting, IP localization, and biometrics contribute to improved risk assessment procedures in customer identification programs. Innovative risk management solutions enable stakeholders such as card issuers, payment service providers (PSPs), and merchant acquirers to analyse data from various channels effectively.

Regulatory compliance is paramount, as major card associations like Visa and MasterCard impose strict rules and regulations on their principal members. Non-compliance can result in heavy fines, penalties, and termination of partnerships. Implementing intelligent and innovative risk management and fraud prevention programs is essential for all stakeholders involved in the online payments business to mitigate financial losses and protect against reputational damage.

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. Implementing intelligent and innovative risk management and fraud prevention programs is essential for all stakeholders involved in the online payments business to mitigate financial losses and protect against reputational damage.

Countering fraud

«Today, EFM solutions are real-time data ingestion platforms that must respond to payment fraud management requirements (account-to-account transfers) with instantaneous risk-scoring engines. EFM solutions must be able to intercept fraudulent transactions in real time. Payments are multifaceted and dictate that the EFM solution offers a highly



	Global average	UK & Ireland	USA	Canada	Australia	France	Germany	Italy	Spain	Mexico	Brazil
● Rules	45%	38%	45%	44%	45%	53%	40%	47%	45%	41%	54%
● Machine learning	48%	46%	44%	58%	58%	50%	49%	51%	49%	40%	38%
● Graph networks	30%	18%	20%	33%	40%	31%	30%	28%	34%	40%	31%
● Device ID solution	53%	51%	57%	55%	53%	46%	52%	52%	51%	54%	60%
● Two factor authentication (2FA)	61%	75%	66%	55%	58%	58%	61%	67%	51%	56%	56%
● Consortium data	20%	20%	22%	20%	22%	23%	24%	17%	18%	27%	12%
● Behavioural biometrics	40%	51%	45%	35%	25%	39%	43%	35%	41%	41%	49%

Source: Ravelin, Global Fraud Trends; Fraud & Payments Survey 2023,

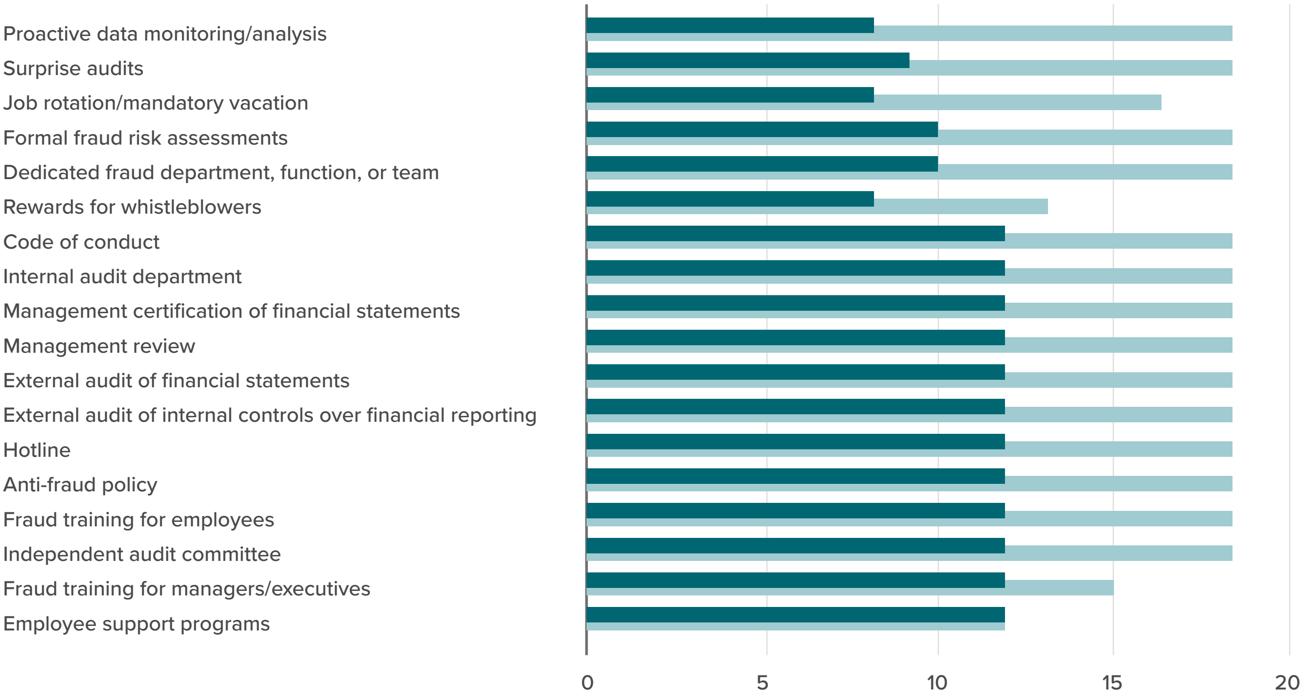
flexible data schema, as well as the ability to participate in data federation with core banking systems across multiple areas (including ATM, ACH/wire, and online bill pay).» Andres Czer

The recent report by Ravelin[11] underscores the enduring effectiveness of various fraud prevention tools when utilised correctly. The analysis suggests that despite the evolving nature of fraudulent activities, existing tools and strategies can still provide robust defence mechanisms against fraudulent behaviour. This assertion implies that with proper implementation and optimization, businesses can continue to leverage these tools to effectively combat fraud, safeguarding their operations and financial interests. Notably, Two-Factor Authentication (TFA) emerges as one of the most effective tools, with over 50% effectiveness reported in each of the surveyed regions.

The presence of an anti-fraud solution has been proven to reduce the median duration of fraud within organisations by an average of 40% in various cases.

[11] Ravelin, in their "Global Fraud Trends; Fraud & Payments Survey 2023,"

How does the presence of anti-fraud controls relate to the duration of fraud?

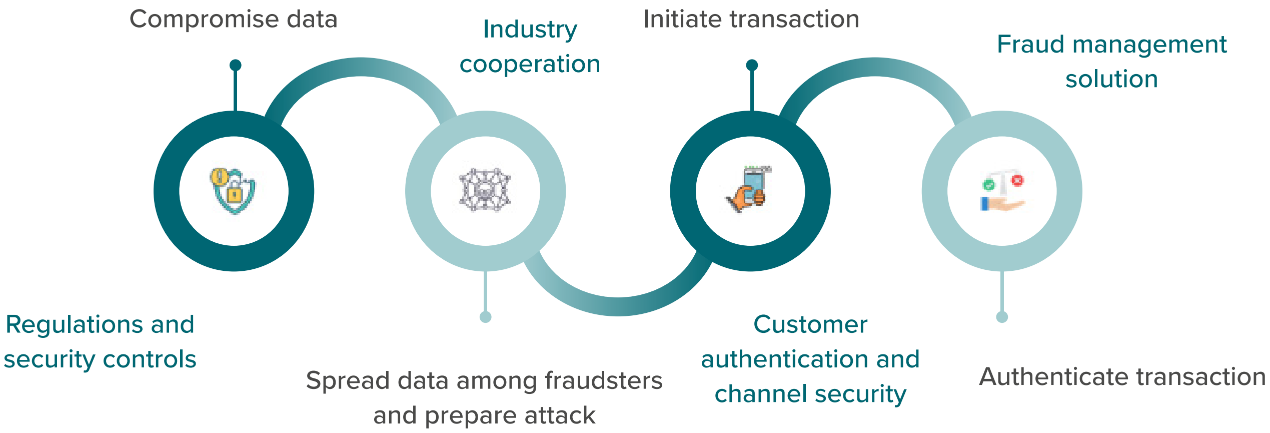


Source: Source: Ravelin, Global Fraud Trends; Fraud & Payments Survey 2023

Furthermore, there has been a noticeable shift in organisational strategies towards strengthening fraud management capabilities, with companies willing to increase operational expenditure for fraud management by an average of 15% within the next two years. This trend clearly indicates that businesses are acknowledging the importance of enhancing their defences against fraudulent activities. Moreover, this trend aligns with a broader industry movement towards adopting customer-centric enterprise fraud frameworks. By prioritising investments in robust fraud management solutions and embracing a customer-centric approach, organisations aim to not only mitigate financial risks but also enhance customer trust and loyalty, thereby positioning themselves advantageously in the market.

In addition to that, according to a survey conducted by Datos-Insights[12], 58% of AML (Anti-Money Laundering) executives believe that KYC (Know Your Customer) and advanced analytics are crucial for developing more informed customer risk profiles and shaping AML monitoring, investigation, and detection efforts.

[12] https://datos-insights.com/reports/top-10-trends-in-risk-2024-unleashing-innovation-against-the-rising-threat-landscape/


Compromise data
Industry cooperation
Initiate transaction
Fraud management solution
Regulations and security controls
Spread data among fraudsters and prepare attack
Customer authentication and channel security
Authenticate transaction

In 2021, ACAMS, in their "The Convergence of Cyber, Fraud, and AML" whitepaper, emphasised addressing the intersection of cyber threats, fraud prevention, and Anti-Money Laundering (AML) activities. They proposed the implementation of a "fusion shell approach," advocating for the establishment of a Fusion Cell comprising representatives from key areas such as Cyber, Fraud, and AML. Additionally, they suggested considering the inclusion of other relevant departments like Information Technology, Sanctions, Legal, and Advisory to ensure comprehensive coverage.

Countering fraudulent activities necessitates a systematic approach starting with the establishment of stringent regulations and security controls. Regulatory compliance lays the foundation for effective fraud prevention by ensuring adherence to standards and guidelines for enhanced security measures. Additionally, industry collaboration among institutions is crucial, enabling the exchange of insights and resources to collectively address threats.

Prioritising strong customer authentication, including robust Know Your Customer (KYC) protocols, and employing channel security technologies are necessary steps. By leveraging appropriate technology, organisations can bolster authentication processes, safeguarding sensitive transactions and data from unauthorised access. The implementation of tailored fraud management solutions tailored to the unique requirements of each business is essential to deploy advanced analytics and detection capabilities to proactively identify and mitigate fraudulent activities.

Chapter 06

Use cases

06

DSK Bank, Bulgaria

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 Fraud Management 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 r isk 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.

Banca Transilvania, Romania

The Bank

Banca Transilvania, hailed as one of Romania's leading financial institutions, has rapidly escalated its presence in the digital banking sphere. With an increase in its card volumes to 6 million, Banca, they recognised the importance of safeguarding its customers' transactions, the bank has embarked on a journey to combat card fraud

The challenge

Banca Transilvania was determined to protect its customers from fraud across all its services, including issuing cards, processing payments, and online transactions. Recognizing the increasing risks in the digital landscape, the bank invested in top-notch security measures. By upgrading its systems and protocols, Banca Transilvania aimed to ensure that every interaction, whether in-store or online, was safe and secure for its customers. This proactive approach not only mitigated risks but also enhanced trust in the bank's services, reassuring customers of their financial security.

The solution

Banca Transilvania chose BPC to boost security across its payment operations, particularly focusing on card issuing, CNP and acquiring channels. BPC's solution provided risk-based analysis tailored for 3DS2 compliance, ensuring transactions met the latest security standards. Additionally, it ensured compliance with PSD2 regulations, enhancing customer trust while meeting regulatory requirements. This move underscored Banca Transilvania's commitment to providing secure and reliable banking services to its customers.

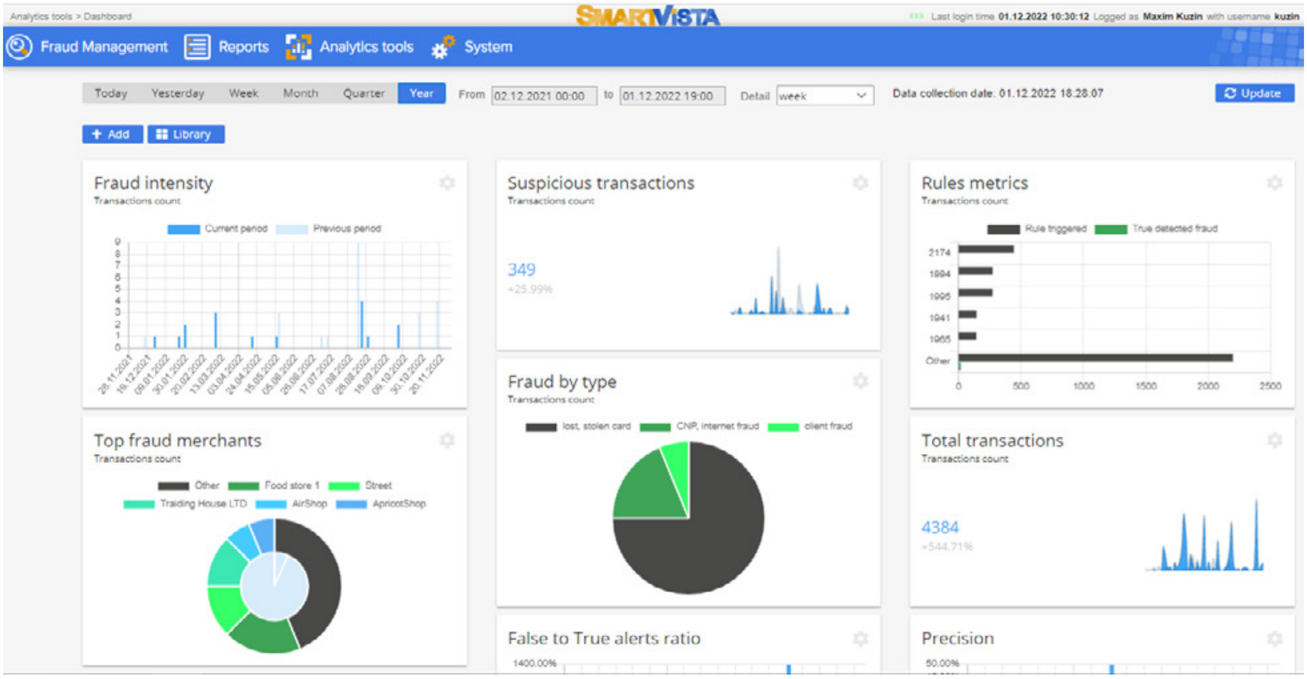
The result

Banca Transilvania saw significant success with the implementation of customizable rule configurations, empowering the bank to align strategies with internal policies effortlessly. The introduction of intuitive dashboards facilitated seamless rule visualisation, functionality testing, and real-time tracking, resulting in a substantial reduction in fraudulent activities.

SmartVista Fraud Management Solution

Fraud is an inevitable challenge in the business landscape, but at BPC, we're dedicated to embedding fraud prevention as a core aspect of our offerings. Leveraging a real-time approach, we address fraud comprehensively across all entities in the payment chain and through every channel, while continuously updating your dashboard with live data.

BPC's Fraud Management solution empowers issuers, acquirers, and other financial entities to detect and prevent fraud across all payment channels instantly. The SmartVista Fraud Management solution specialises in real-time transaction monitoring and enables detailed statistical profiling at every level – whether it's card, terminal, merchant, device, account, customer or institution.



Analytics tools > Dashboard

Last login time 01.12.2022 10:30:12 Logged as Maxim Kuzin with username kuzin

Year

From 02.12.2021 00:00 to 01.12.2022 19:00

Detail week

Data collection date: 01.12.2022 18.28.07

Your options:

- Enjoy end-to-end service [SaaS]: Access our comprehensive service hosted in the cloud for a hassle-free experience.
- Make it your way [on-premise]: Opt for an on-premise solution for full control and customization according to your specific needs.

SmartVista Fraud Management is equipped with an advanced analytical tool and a robust, business-driven rules engine. It scrutinises each transaction against a bespoke set of business rules, capable of monitoring an extensive array of parameters. These range from basic checks, like transaction location, to more complex validations based on the historical profile of the card or account involved.

Key features:

- Risk-based and transaction-based authentication: Implement RBA and TBA methods to fortify security measures, providing authentication codes with every transaction to ensure utmost security.
- Advanced alert features: Receive immediate notifications of any suspicious activity, enabling prompt action to prevent potential fraud.
- Comprehensive coverage: Our services extend across multiple institutions, offering a unified view of your entire business landscape.

Powered by advanced Machine Learning and Neural Network models, the SmartVista Fraud Management solution simplifies complex data analysis. This facilitates a secure and intelligent payments ecosystem for financial institutions and their clientele.

Organisations can delve into transactions with a 360-degree customer view across all channels. Real-time monitoring ranges from online card usage to core banking transactions, allowing for the creation of precise customer profiles based on common behaviour patterns.

By analysing account transaction history to assess the risk level of each transaction, additional security measures can be applied as necessary. This approach not only ensures the maximum security for your customers but also builds a strong trust foundation, critical in today's digital age.

In essence, the SmartVista Fraud Management solution represents BPC's commitment to pioneering in the field of fraud prevention, offering flexible, robust solutions that cater to the diverse needs of the modern financial services industry.

About BPC

BPC

Founded in 1996, BPC is a proven industry leader that is shaping the world of transactions with quick, safe and easy payment processing. With a focus on exceptional technology development and customer service, BPC helps financial institutions and businesses to deliver innovative and best-in-class proven solutions that fit with today's consumer lifestyle when banking, shopping, or moving in both urban and rural areas.

With more than 450 customers across 120 countries, BPC collaborates with all ecosystem players to deliver services for the digital world.

Its core product SmartVista suite comprises cutting-edge banking, commerce, and mobility platforms that enable innovative solutions for digital banking, ATM and switching, payments processing, card, and fraud management, financial inclusion, merchant portals, transport, and smart cities. To find out more about how BPC can help businesses deliver a seamless payments processing experience to consumers, please visit **www.bpcbt.com**

BPC