Is This The Calm Before The Storm?

After two years of rising, fraud seems to be flattening. But are AI-powered fraudsters merely retooling for the next phase?

The LexisNexis® Risk Solutions Cybercrime Report

TABLE OF CONTENTS

2025 Edition
Based on analysis of data from January to December, 2024

Introduction

After several years of skyrocketing digital fraud (as tracked through LexisNexis® Digital Identity Network® solution), data shows the rate of attacks by humans rising by just 1% last year. That said, the number of attacks is still increasing, and organisations that become complacent are putting themselves at risk. Challenges are still multiplying around the world, and in the communications, mobile and media sector attack rates were up 15% year-over-year (YOY). In other sectors, there was no significant increase in attack rate, suggesting that fraudsters are avoiding organisations with more sophisticated defences.

But the attack-rate slowdown we're seeing might be short-lived; fraudsters and scammers are likely retrenching against heightened security. In this report, we explore the tangled web of scams and mules in depth, and show how our data reveals tell-tale patterns of scam and mule activity. And we'll demonstrate the value of collaboration as the only way to reliably reduce fraud in today's complex environment.

Scams dominate global headlines, but organisations today struggle with a wide range of attacks, including the use of compromised or synthetic identities and payment credentials, bonus abuse and first-party fraud. In our detailed look at the relative incidence of these fraud classifications, first-party fraud was the number one reported category.

On the other side of the equation, enterprises that have invested in modern, sophisticated defences are enjoying success. AI tools are rapidly improving and scaling existing fraud detection schemes, for example by enriching data sets with additional context to better identify unusual behavioural correlations that may signal fraud. Collaboration and data-sharing frameworks are important and growing practices as well, helping member organisations share intelligence on fraudulent entities and linking fraudsters in recognisable patterns of attack. As organisations overcome their hesitation to collaborate (often due to regulatory complexity and/or privacy laws), they're drawing more value from their fraud detection solutions. Around the world, revisions of regulatory frameworks (like PSD3) are starting to provide improved clarity.

Ongoing concern about fraudsters using generative AI has, so far, been limited to a relatively small number of well-reported cases that have required a fair amount of planning and sophistication (and human intervention). We do expect AI-powered fraud to grow and evolve; we're already detecting more frequent usage in new account origination attempts to defeat less-robust document authentication checks. Having a flexible, multi-layered fraud prevention strategy has never been more critical, so organisations can adjust their defences as needed to meet these ever-evolving threats.

In addition to trends and analysis from the Digital Identity Network® solution, several specific topics will be explored further, including:

- Behavioural Intelligence
- Refining Trust with AI
- UK Liability Changes With Potential For Global Impact
- Collaboration and Consortia

Global Risks

Current Analysis

LexisNexis® Risk Solutions analysed more than 104 billion transactions for this Cybercrime Report - a new record. We found that, after two years of substantial increases, overall global attack rates finally began stabilising. Here are the details.

Global Highlights

By Transactions

All events analysed in the Digital Identity Network solution

- +13% Global transaction volume year-over-year (YOY)
- +16% Financial Services transactions
- -1% Ecommerce transactions
- +5% Communications, Mobile and Media transactions
- +7% Gaming and Gambling transactions

By Human-Initiated Attacks

Events where the attacker is human

- +1% Human-initiated attack rate YOY
- +3% Financial Services attack rate
- +1% Ecommerce attack rate
- +15% Communications, Mobile and Media attack rate
- -9% Gaming and Gambling attack rate

Automated Bot Attacks

Events where the attacker is code

- -15% Automated bot attacks YOY
- +18% Financial Services bot volume
- -59% Ecommerce bot volume
- +5% Communications, Mobile and Media bot volume
- -4% Gaming and Gambling bot volume

Attacks analysed in the Digital Identity Network® solution are divided into attacks by humans, which typically return full digital identity profiling data relating to individual events, and high-velocity automated bot attacks.

Global Transaction Patterns, by the Numbers

A new milestone is reached in annual transactions analysed by LexisNexis® Risk Solutions

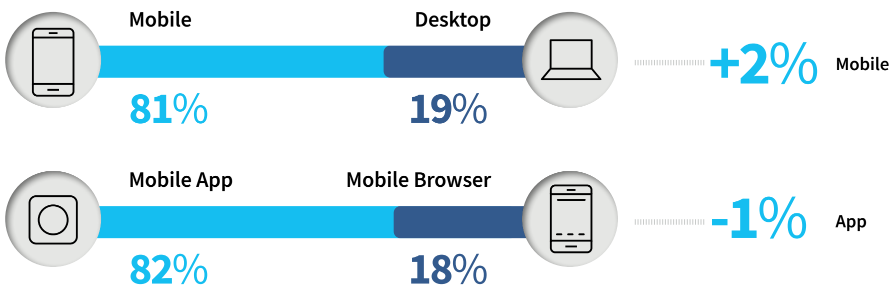
We analysed more than 100 billion transactions in Digital Identity Network solution for this report, an increase of 13% YOY. What we found by assessing all this data is that the worldwide shift from desktop to mobile continues to mature, with the times of double-digit growth receding into the past. And of those mobile transactions, more than four out of five are conducted on a mobile app, versus a traditional browser, though that share of mobile apps has actually shrunk slightly (down 1% YoY).

We saw double-digit growth in transactions across all three primary use cases for customers: new account creations, logins, and payments, showing a similar distribution to the previous year's data. New account transaction growth slowed in 2022 after a prior explosion, then re-emerged again last year as a driver of overall transaction growth.

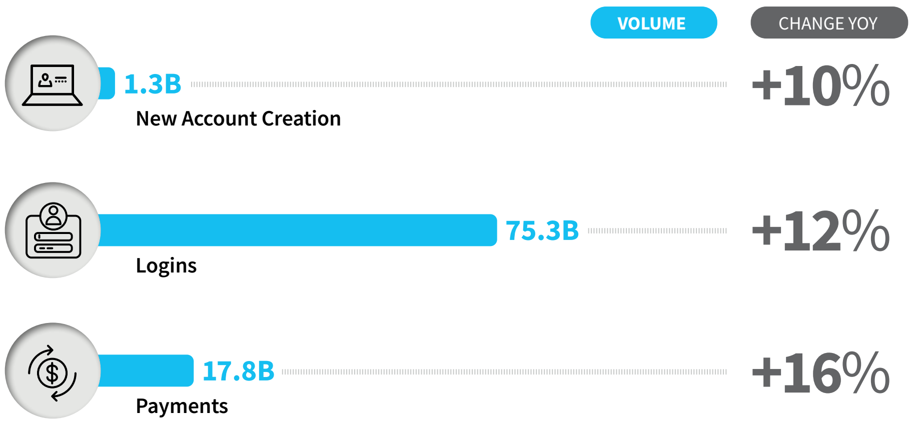
Digital Identity Network now analyses more than **100 BILLION** transactions per year.

104.1B
+13%

TRANSACTIONS BY CHANNEL



TRANSACTIONS BY USE CASE



Global Attack Patterns, by the Numbers

Overall attack rates stabilise, but remain at historically high levels

The overall rate of attack by humans is 1.5%, up modestly 1% YOY. Nearly three quarters of these attacks came from mobile devices, a slight increase. It's possible that attack volume may have reached a plateau, where any further effort is producing a diminishing rate of monetary returns, though cybercriminals' increasing use of AI may move this threshold more in the fraudsters' favour going forward.

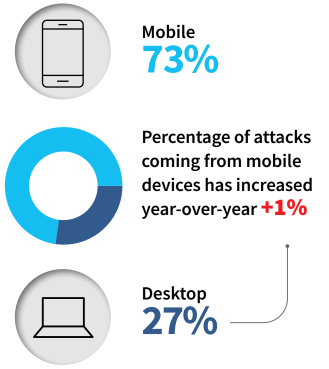
No significant changes in attack rates were seen across the different channels—mobile browser-based traffic remains the clear leader in risk, followed by desktop browsers. Mobile browsers are generally considered the least secure channel due to their lightweight nature, which limits the amount of digital intelligence available to detect fraud. From a pure volume standpoint, the majority of actual attacks are now occurring via the mobile app channel, showing that mobile app traffic needs to be more effectively risk assessed. It is also likely that fraudsters are focusing more of their attacks on less well protected digital services not seen by the Digital Identity Network.

Automated bot attacks fell significantly (down 15% YOY), led by ecommerce after that industry sustained elevated levels during the two previous years. The focus of bot attacks shifted instead to financial services, where more than two-thirds of all detected bots were seen. Globally, financial services bot traffic was up 18%, driven by an increase of 22% in North America specifically.

3.1B
CHANGE YOY
-15%

HUMAN-INITIATED ATTACKS

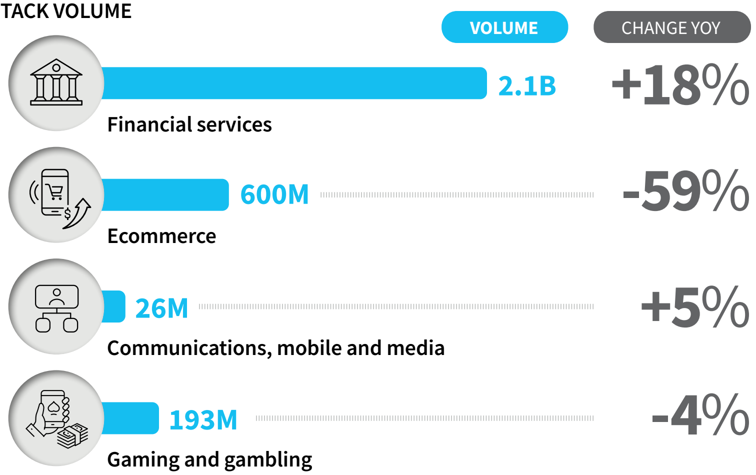
ATTACK VOLUME



ATTACK RATE		CHANGE YOY
OVERALL	1.5%	+1%
DESKTOP	2.1%	+6%
MOBILE BROWSER	3.9%	+4%
MOBILE APP	0.8%	-6%

AUTOMATED BOT ATTACKS

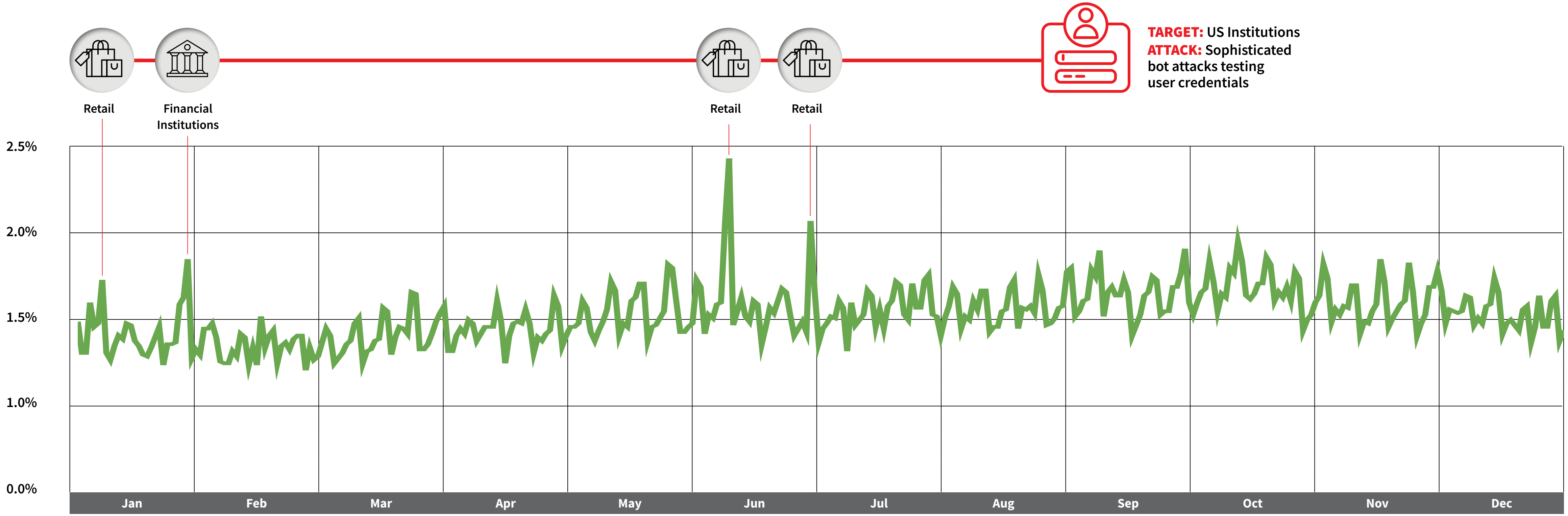
ATTACK VOLUME



Identity Abuse Index

Is this merely a calm before the storm?

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day across the entire Digital Identity Network solution, including both human-initiated and sophisticated bot attacks. This index was relatively stable this year, showing little sustained growth YOY (1%), as concerns about increased threats linked to AI have so far proved unfounded. However, fraudsters' initial focus may have been on testing these new technical capabilities with smaller attacks, and we may see AI drive up attack rates in next year's data. An analysis of attacks over a longer period (5+ years) shows they often come in waves—with a plateau preceding the arrival of the next wave.



TARGET: US Institutions
ATTACK: Sophisticated bot attacks testing user credentials

Scammers, Victims and Mules: How The Deception Works

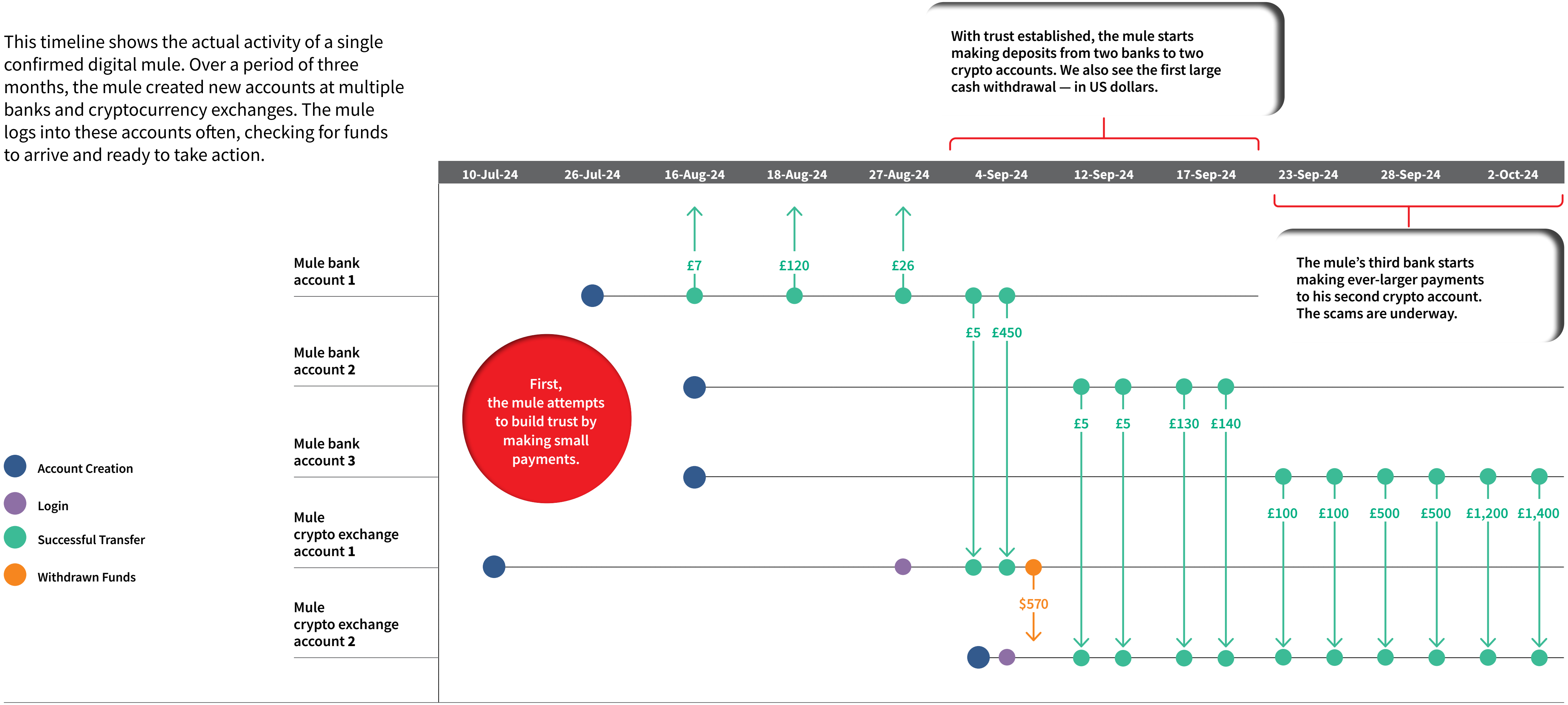
For an authorised push payment scam to succeed, there must be a financial beneficiary account prepared to receive the victim's funds. The money mule who controls this account then rapidly disperses funds to additional mule accounts, often in parallel, making it incredibly difficult for anyone to follow the flow of money. Mule accounts support a deeply concerning rise in scams around the world.

In the UK, where scams first made headlines years ago, mule-related money movements seen in the Digital Identity Network solution are up 65% YOY.

On the following pages, we share a few deep dives into typical scam and mule activity using real-world data and insights generated by the Digital Identity Network solution. These are peeks into actual data, showing some common scam patterns from a few different viewpoints—only the identifying details have been anonymised.

View 1 The Mule Sets Up Shop

This timeline shows the actual activity of a single confirmed digital mule. Over a period of three months, the mule created new accounts at multiple banks and cryptocurrency exchanges. The mule logs into these accounts often, checking for funds to arrive and ready to take action.

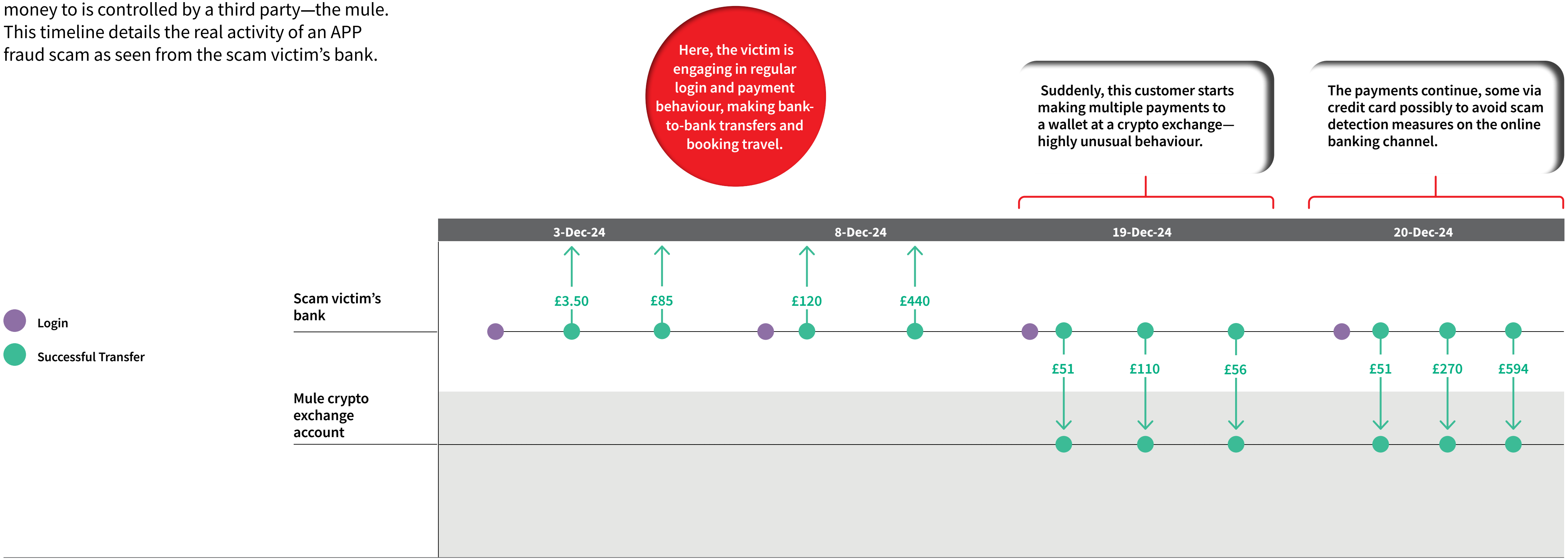

With trust established, the mule starts making deposits from two banks to two crypto accounts. We also see the first large cash withdrawal — in US dollars.

First, the mule attempts to build trust by making small payments.

The mule's third bank starts making ever-larger payments to his second crypto account. The scams are underway.

View 2 A Scam Victim's Bank Activity

In an authorised push payment fraud (APP), the victim is convinced to move money out of their bank account and into someone else's. Of course they don't know they're being scammed, but they also don't know the account they're moving the money to is controlled by a third party—the mule. This timeline details the real activity of an APP fraud scam as seen from the scam victim's bank.



Here, the victim is engaging in regular login and payment behaviour, making bank-to-bank transfers and booking travel.

Suddenly, this customer starts making multiple payments to a wallet at a crypto exchange—highly unusual behaviour.

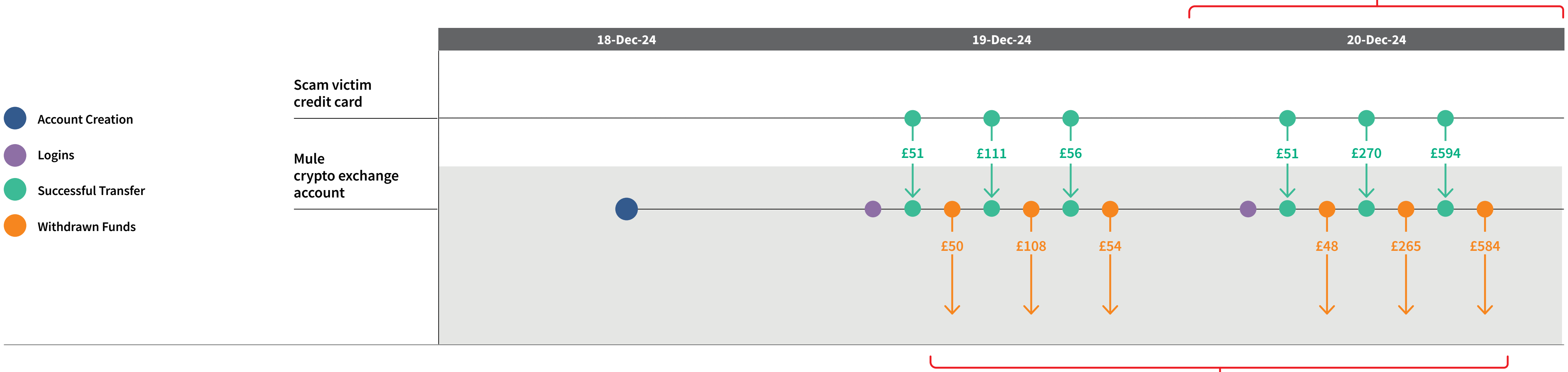
The payments continue, some via credit card possibly to avoid scam detection measures on the online banking channel.

View 3 Suspicious Crypto Activity Heats Up

This view focuses on the activity in the cryptocurrency wallet of a known money mule. We can see the transfers in (from a customer's credit card) and out (funds withdrawn as cash), as well as timing for logins and new-account openings. And it reveals a telltale pattern of fraud.

The mule creates a new wallet at a crypto exchange. Within 24 hours, the scam victim is making deposits into it.

After the final withdrawal, no activity is seen in this crypto wallet. The scam is complete—the money is gone.



The mule logs in constantly. As each payment enters the crypto account, he or she withdraws nearly all of it minutes later.

View 4 Mules Take Their Activity Worldwide

These scams happen around the world every day, as victims deposit money in mule accounts and mules quickly hide that money or cash out through cryptocurrency exchanges or online gambling sites. The networked activity on this page hints at the extent of the challenge for financial institutions, cryptocurrency exchanges, gaming and gambling operators and law enforcement.

The arrows represent confirmed mules spotted first at one organisation and moving to a different institution, creating new mule accounts, checking on funds received or initiating further fund transfers.

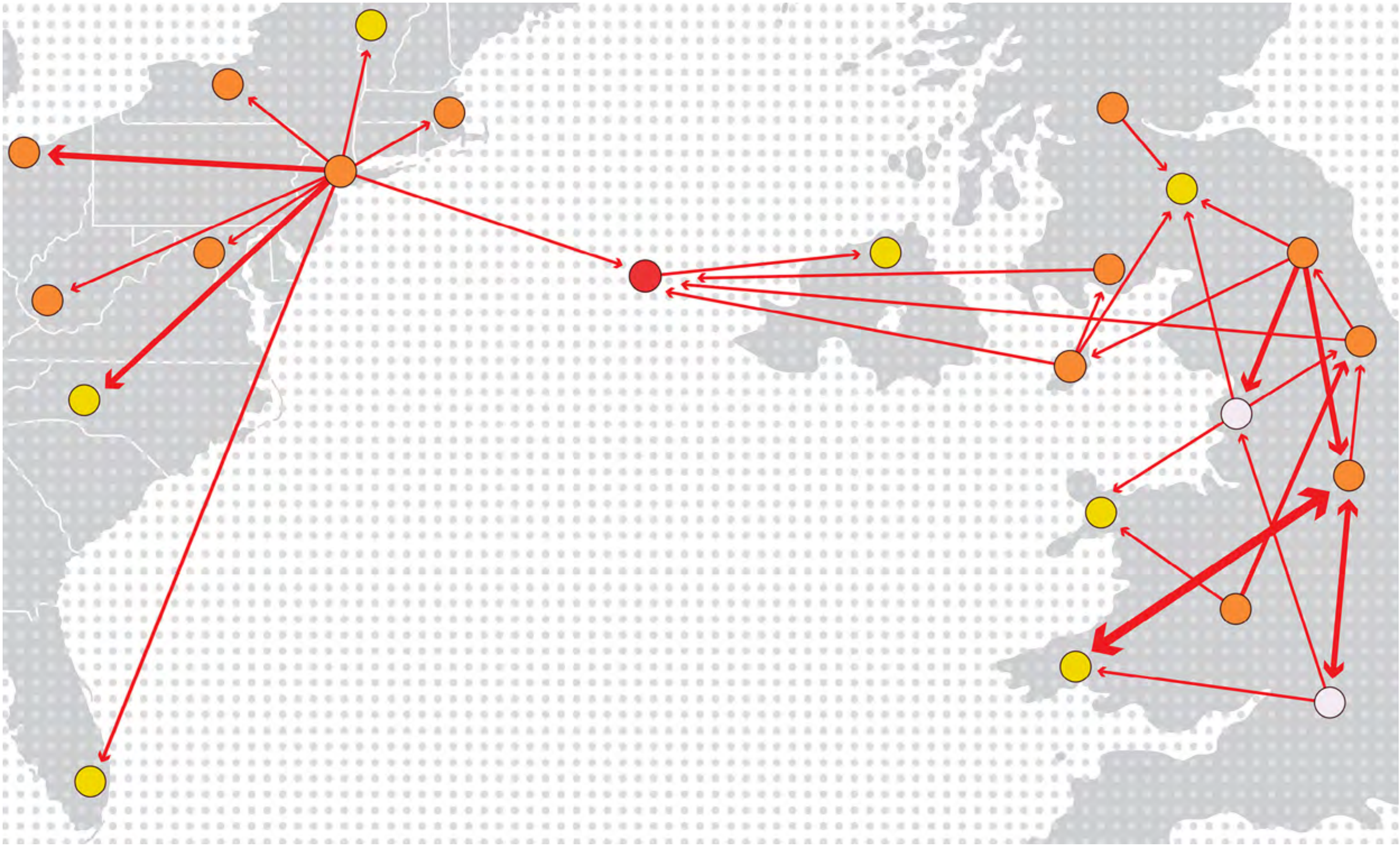
Mules often operate within a country's borders to reduce chances of detection (as seen here in the clusters within the UK and US). But they also operate across borders, for example cashing out with cryptocurrency exchanges, facilitating a global operation of illicit money movement that's hard to track.

● Financial Service

○ Digital Bank

● Gaming and Gambling

● Crypto Wallet



Locations have been changed to anonymise the institutions involved.

Fighting Back: How Businesses Are Solving This Challenge

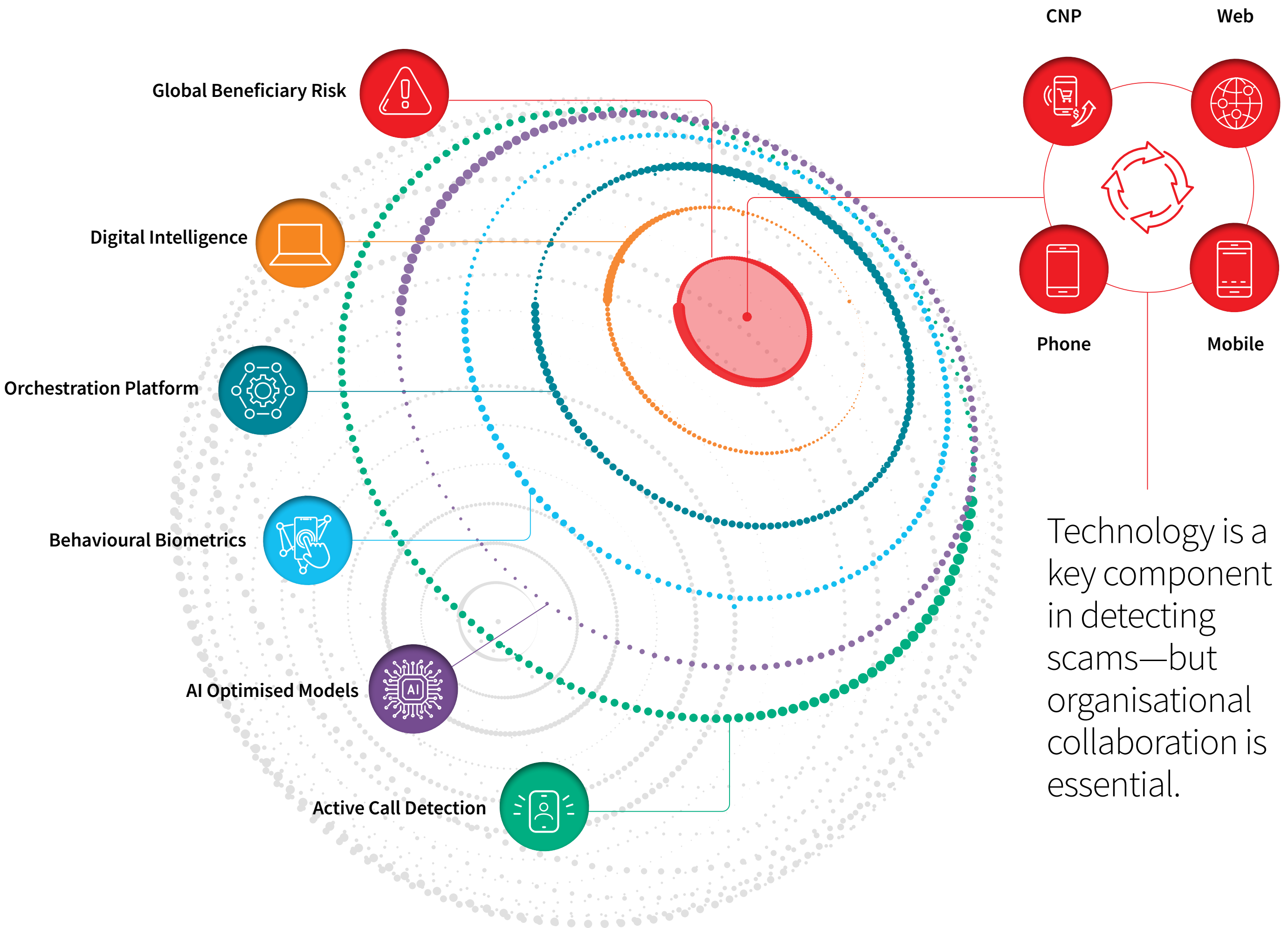
Detecting APP fraud requires a comprehensive, multi-layered approach, bringing together data, analytics and a broad understanding of the evolving scam landscape. Successful results often involve:

- **Connecting money flow analysis to digital intelligence, to enable richer, multi-dimensional data analysis**
- **Using AI to optimise detection models that can extract multiple fraud and mule signatures out of the same data**
- **Expanding data intelligence beyond a single organisation's view by collaborating through fraud prevention consortiums**

How well a model works depends on a number of factors, including a bank's ability to review alerts and their ability to fully leverage all available data. But optimised models across our global banking clients have produced APP fraud detection rates of 40 to 70 percent.

Customer education is key, and organisations can introduce targeted messaging that discusses scam scenarios. They can also block high-risk payment attempts, and deploy a trained operations team to reach out to customers to validate any payments deemed risky.

While technology can go a long way to helping to detect scams, it's just one part of a community approach where businesses and law enforcement work together with the general public to succeed.



Technology is a key component in detecting scams—but organisational collaboration is essential.

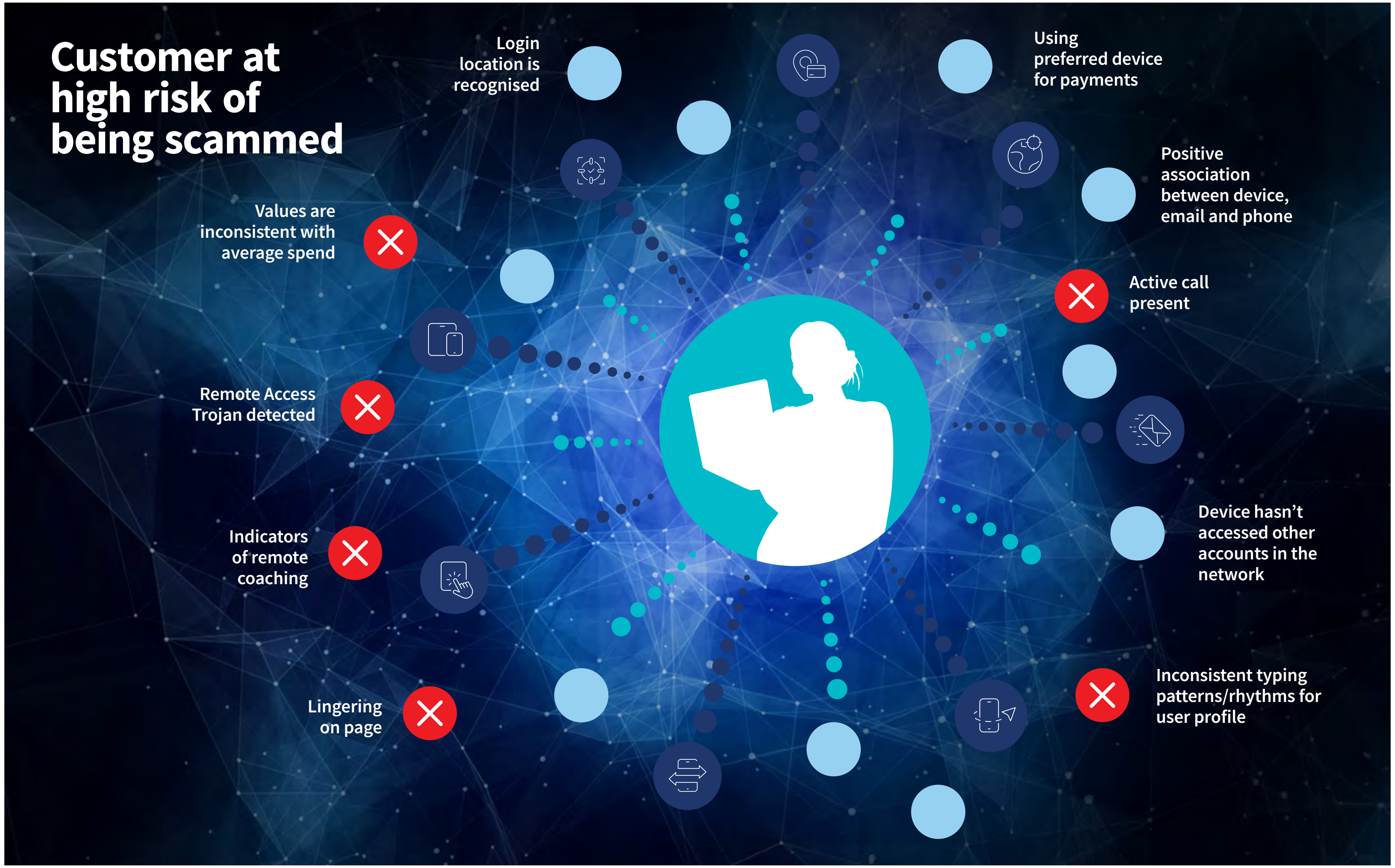
Fighting Back: Collecting Behavioural Intelligence for an Extra Layer of Protection

As fraud evolves and becomes more complex, it's more vital than ever for organisations to bring in as much data as possible to contextualise each event and assess its risk.

Many financial institutions are adding an additional layer of behavioural biometrics technology to their fraud defences. This technology can range from simple flags indicating the use of cut and paste or basic models calculating a risk score, up to more nuanced indicators of the evidence of bots, coaching a victim or advanced AI-based models. This technology can also reduce false positives by building trust with known users, or identifying anomalies from normal behaviour based on user or population profiling.

This technology can also be used beyond financial institutions. It's particularly useful for detecting synthetic identities during new account openings, and for identifying social engineering and coaching signals during payments.

Adding behavioural biometrics to existing fraud prevention technology utilising the Digital Identity Network solution typically shows between a 10 to 30% uplift in model performance. This can reduce mistaken manual reviews, detect more scams, or both.



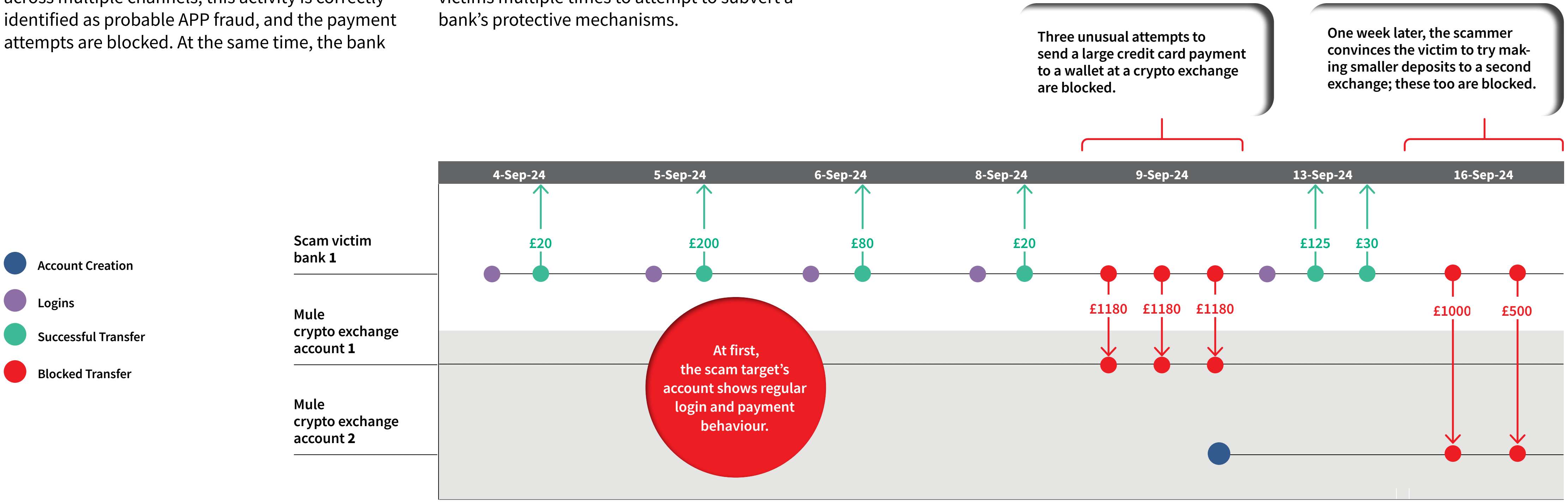
Customer at high risk of being scammed
Login location is recognised
Using preferred device for payments
Values are inconsistent with average spend
Positive association between device, email and phone
Active call present
Remote Access Trojan detected
Indicators of remote coaching
Device hasn't accessed other accounts in the network
Lingering on page
Inconsistent typing patterns/rhythms for user profile

Final View How A Proper Fraud Defence Looks

Banks that have optimised their anti-fraud practices are in a much better position to help protect their customers from becoming victims of APP fraud. This timeline shows how strong fraud detection algorithms can help foil APP fraud.

Because this bank is using holistic fraud detection across multiple channels, this activity is correctly identified as probable APP fraud, and the payment attempts are blocked. At the same time, the bank doesn't prevent the customer's normal transactions with legitimate parties.

This example highlights the enhanced ability of the bank to stop these types of attacks when fraud detection models are consistent across channels. It also highlights how fraudsters can engage their victims multiple times to attempt to subvert a bank's protective mechanisms.



Three unusual attempts to send a large credit card payment to a wallet at a crypto exchange are blocked.

One week later, the scammer convinces the victim to try making smaller deposits to a second exchange; these too are blocked.

At first, the scam target's account shows regular login and payment behaviour.

Fighting Back: The UK's PSR Spurs Greater Collaboration

A tectonic shift in the UK fraud regulatory landscape occurred when the Payment Systems Regulator (PSR) began requiring greater reimbursement to the majority of victims of Authorised Push Payment (APP) scams. This step was a world first in raising the standard of consumer protection.

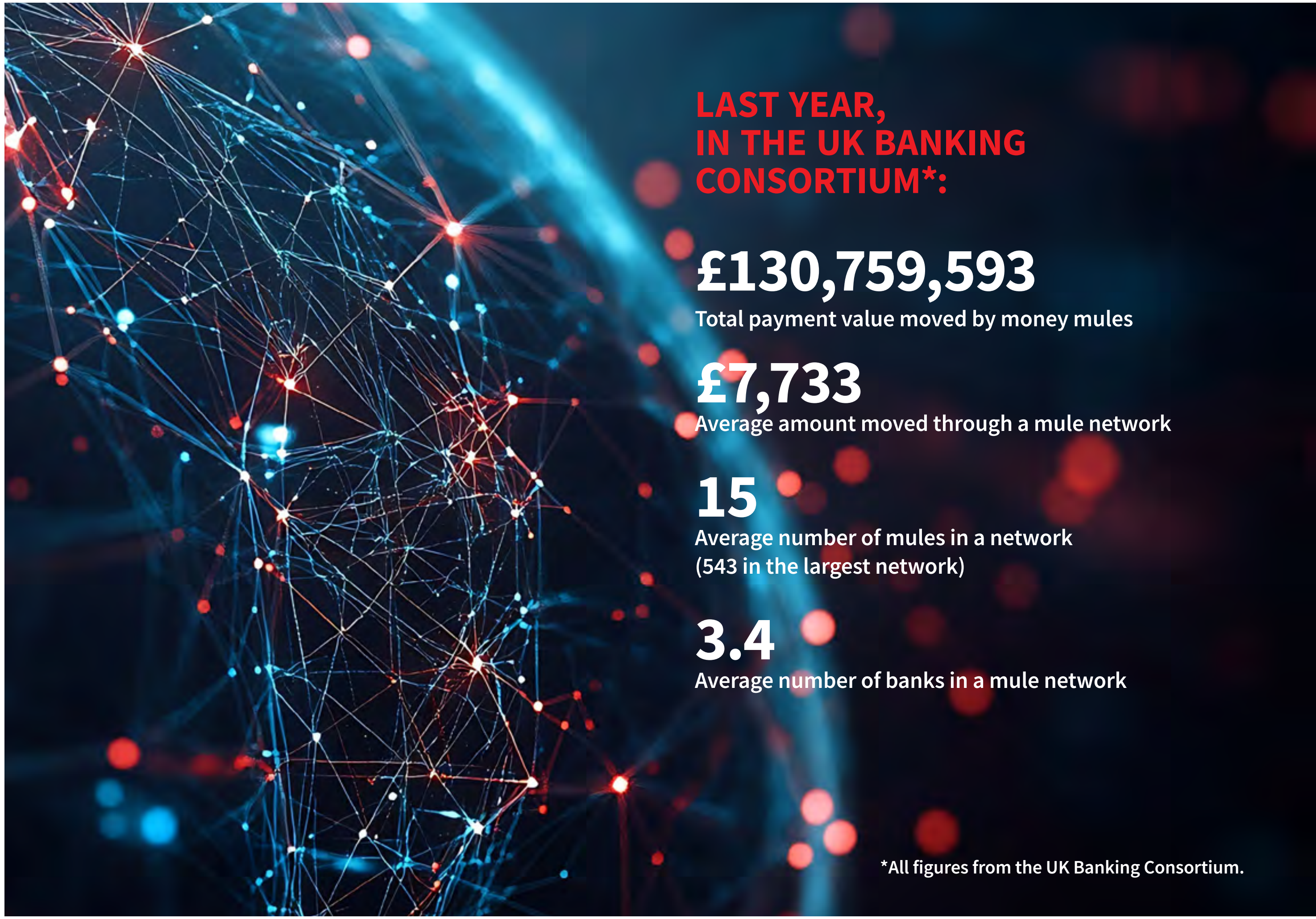
One revolutionary aspect of the PSR change was the introduction of 50/50 liability sharing between the sending and receiving Payment Service Providers (PSPs), up to a maximum reimbursement of £85,000. This new liability model inspired banks to rethink their fraud controls, including assessing the risk of inbound payments to detect potential mules.[1]

To meet these regulations, some of our clients have expanded their use of the Digital Identity Network beyond fraud to mule detection models, and have achieved a 70%+ increase in mule payment detection.

Fraudster behaviour appears to be changing in response to the PSR. Impersonation scams continue to fall, in line with the trend throughout last year. Purchase scams remain high. First-party fraud has increased substantially. Reimbursements are being processed in higher volumes than in the period prior to the PSR's enforced reimbursement.

Other regulators around the world are watching the impact of this change. Some are proposing that telecom operators also share liability. But none are yet following the UK's approach to fully reimburse APP scam victims. The industry has adapted well in raising consumer protection, but fraudster tactics will always evolve.

[1] 'Navigating the Scam Liability Shift' for more on inbound payment risk assessment.



LAST YEAR, IN THE UK BANKING CONSORTIUM*:

£130,759,593
Total payment value moved by money mules

£7,733
Average amount moved through a mule network

15
Average number of mules in a network
(543 in the largest network)

3.4
Average number of banks in a mule network

*All figures from the UK Banking Consortium.

Refining Trust with AI

The smart application of machine learning is boosting fraud detection

Fraud has always been a headache for ecommerce. It can take various forms, such as the use of compromised credit card details, account takeover or refund/return abuse.

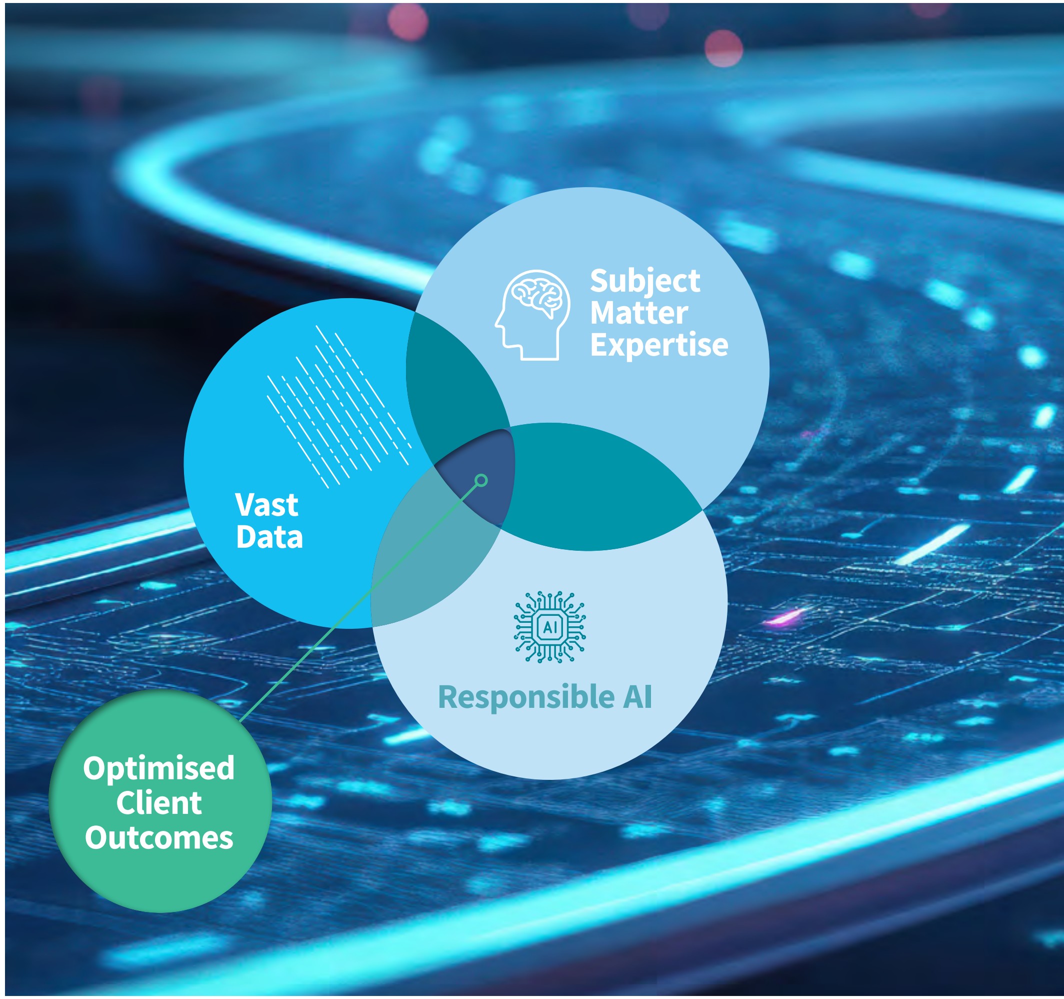
Wider use of strong customer authentication enforced by regulation like Europe's PSD2 can help limit fraud. But it can also affect conversion rates, by increasing customer drop-off. Similar impacts are likely to be seen in Japan in 2025, as 3D Secure becomes a requirement for ecommerce transactions there.

Historically, fraud prevention solutions focused predominantly on detecting signs of fraud. But in recent years it's become clear that identifying good customers and building trust can lead to better results. Using machine learning algorithms to optimise fraud detection models that are focused on building trust with good customers can result in significant improvements.

To succeed, these models should have the following:

- **A highly accessible, rich digital intelligence history, combined with contextual transactional data**
- **An in-depth understanding of the user journey, including cart/basket-level analysis**
- **The ability to differentiate fraudulent versus genuine behaviours, through rich data from across the customer journey and human input to help guide the algorithm**

By implementing these kinds of advanced models, ecommerce merchants have been able to reduce friction or enhance the checkout experience by 60-90% for genuine customers, and fast-track sales worth over $100M annually.



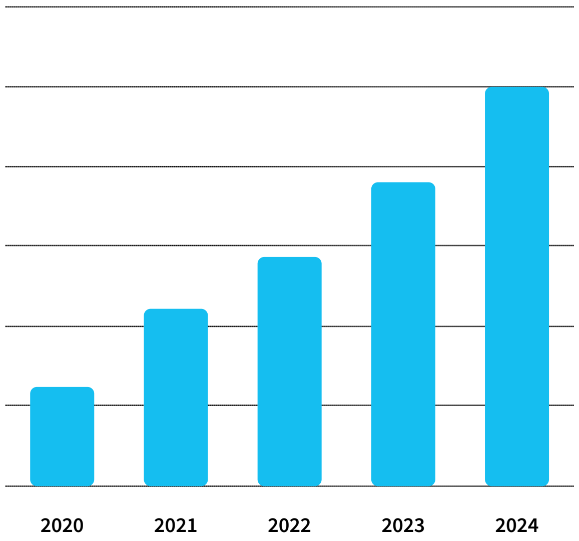
Making the 3D Secure Journey Smarter and Safer

Pushing back against increasing ecommerce fraud

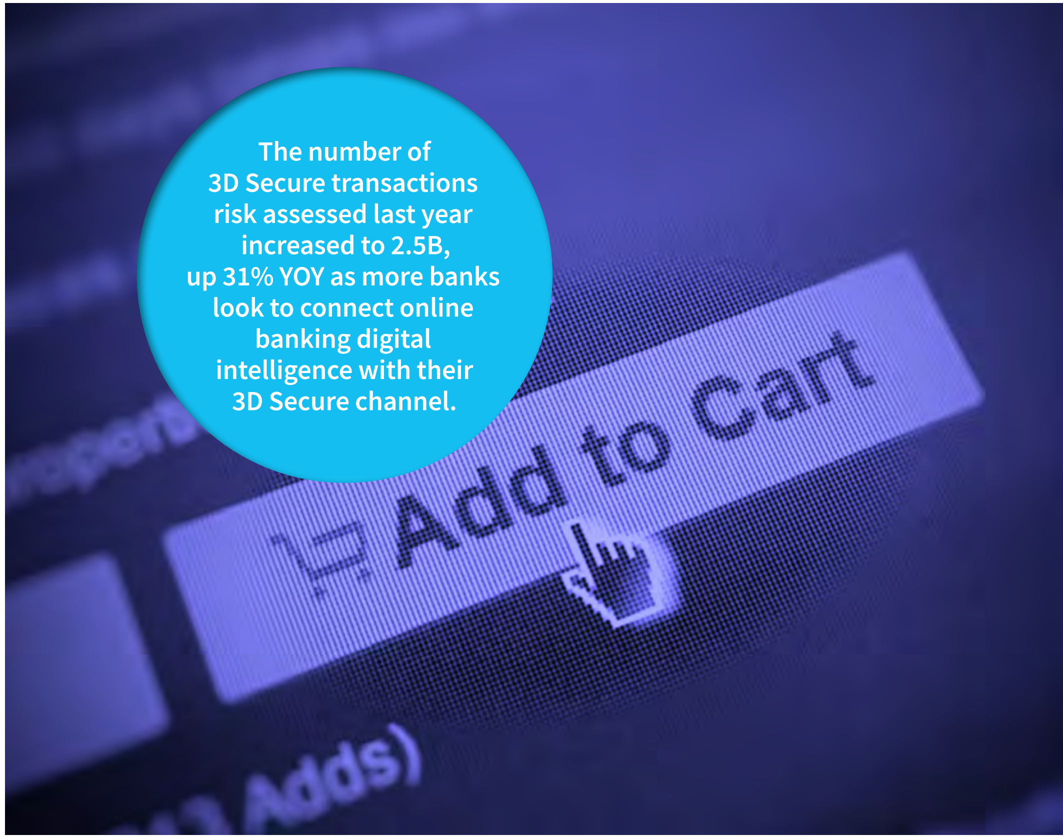
Ecommerce fraud initially declined in Europe, when Strong Customer Authentication was introduced (via 3D Secure). However, that downward trend has now reversed in the UK, with CNP (Card Not Present) fraud again on the rise. This reversal of fortune is likely to increase as time goes on.

What's going on? Scams, a significant problem within the financial services industry for the last several years, are making headway in ecommerce as well. Scammers are convincing victims to share one-time codes or directly authorise fraudulent payments initiated by the scammers, or are even convincing victims to initiate payments themselves, compromising the strong authentication processes being put in place to combat fraud.

Combining fraud models based on digital intelligence with existing 3D Secure ACS provider models can provide extra context and a more consistent, 360° view of a bank's customer base. This has enabled banks to improve CNP fraud detection rates by anywhere from 15% to 100%, preventing up to $1M in fraud losses per month.



3DS TRANSACTIONS



The number of 3D Secure transactions risk assessed last year increased to 2.5B, up 31% YOY as more banks look to connect online banking digital intelligence with their 3D Secure channel.

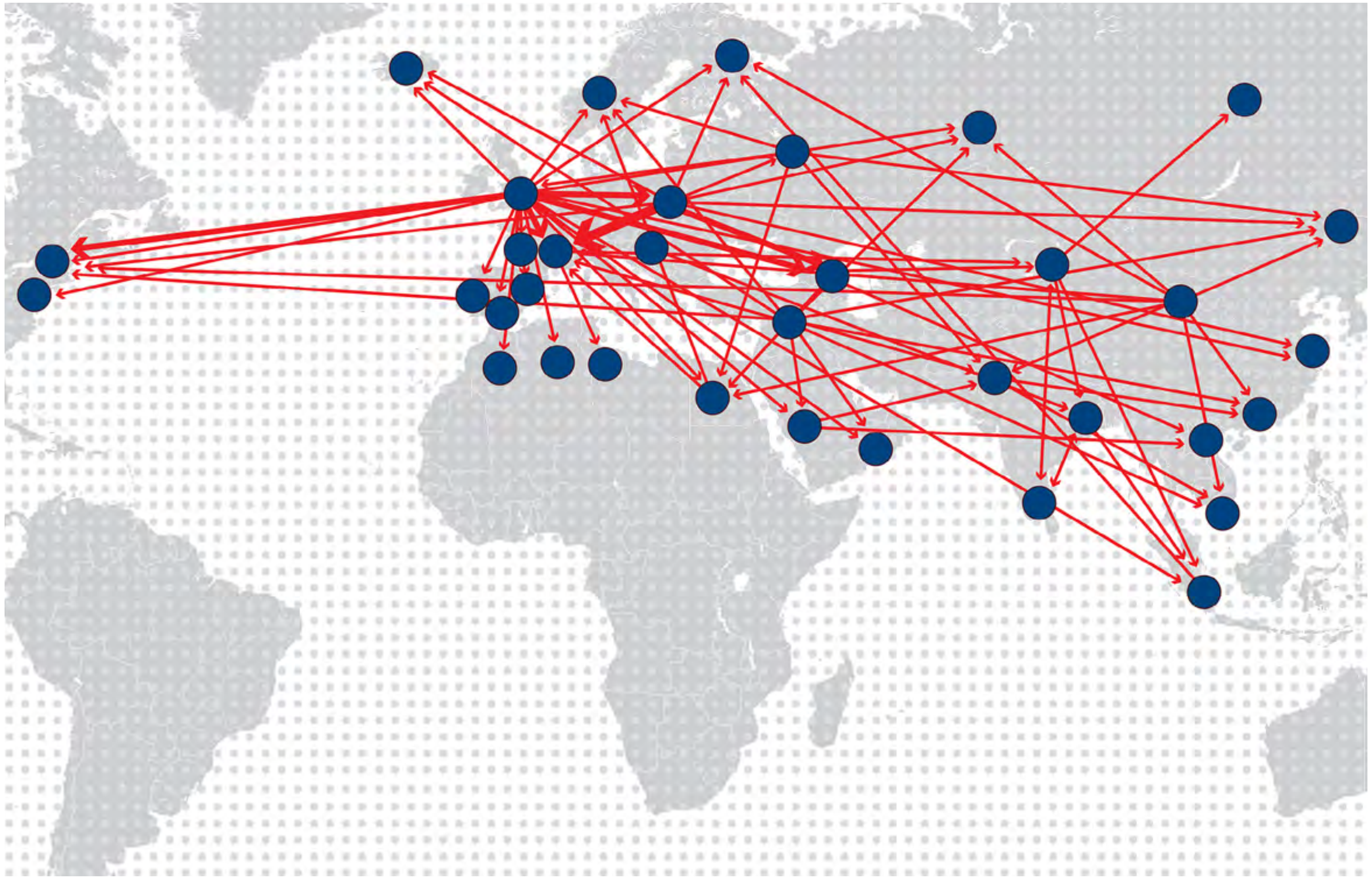
3D Secure Networked Fraud

How credit card fraud spreads freely across national borders

This illustration shows networked payment fraud (linked by digital identity) connected by organisations processing 3D Secure transactions around the globe during the last quarter of last year.

Each circle represents an individual issuing bank processing payments. Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation within Digital Identity Network. A thicker line denotes a higher volume of attacks.

The diagram highlights that when it comes to online credit card fraud, geographical borders or boundaries are meaningless, as fraud networks operate across regions as much as in-region. While perhaps not surprising, as one of the benefits of using a credit card is that they are generally accepted around the world, it highlights the potential power of utilising global digital intelligence to rapidly prevent unauthorised credit card use for organisations looking to accept international card payments.



● Issuing Banks

Locations have been changed to anonymise the institutions involved.

Collaboration and Consortiums

Sharing data and intelligence is emerging as a powerful weapon against fraud

To help organisations prevent repeated fraud attempts, regulators are encouraging collaboration and near-real-time data sharing—but data privacy remains a difficult challenge.

Over the past six years, a growing number of organisations who already benefit from Digital Identity Network have chosen to work even more closely together by enabling consortium capabilities and sharing fraud intelligence with other consortium members. The best of these solutions follow privacy by design, using encryption or pseudonymisation to stay aligned with privacy regulations.

Consortium members share confirmed and suspicious digital intelligence identifiers and payment account details. This collaboration helps with unauthorised fraud, authorised push payment fraud and mule detection.

The proof is in the results: Consortium members report significant increases in fraud value detection rates and up to 2:1 false positive rates on confirmed mule listings when they combine consortium intelligence into their existing detection models.

Consortium members agree to work together more closely and share fraud intelligence.

Consortium Locations No. of members

UK	12	● ● ● ● ● ● ● ● ● ● ● ●
JAPAN	8	● ● ● ● ● ● ● ●
HONG KONG	4	● ● ● ●
SINGAPORE	3	● ● ●
DUBAI	3	● ● ●

Collaboration customers discuss how they fight fraud, share best practices, etc., but do not currently use consortium functionality.

Customer Collaboration Locations No. of members

US	10	● ● ● ● ● ● ● ● ● ●
AUSTRALIA	10	● ● ● ● ● ● ● ● ● ●
FRANCE	8	● ● ● ● ● ● ● ●
POLAND	7	● ● ● ● ● ● ●
CANADA	5	● ● ● ● ●

Fraud Types from a Client Perspective

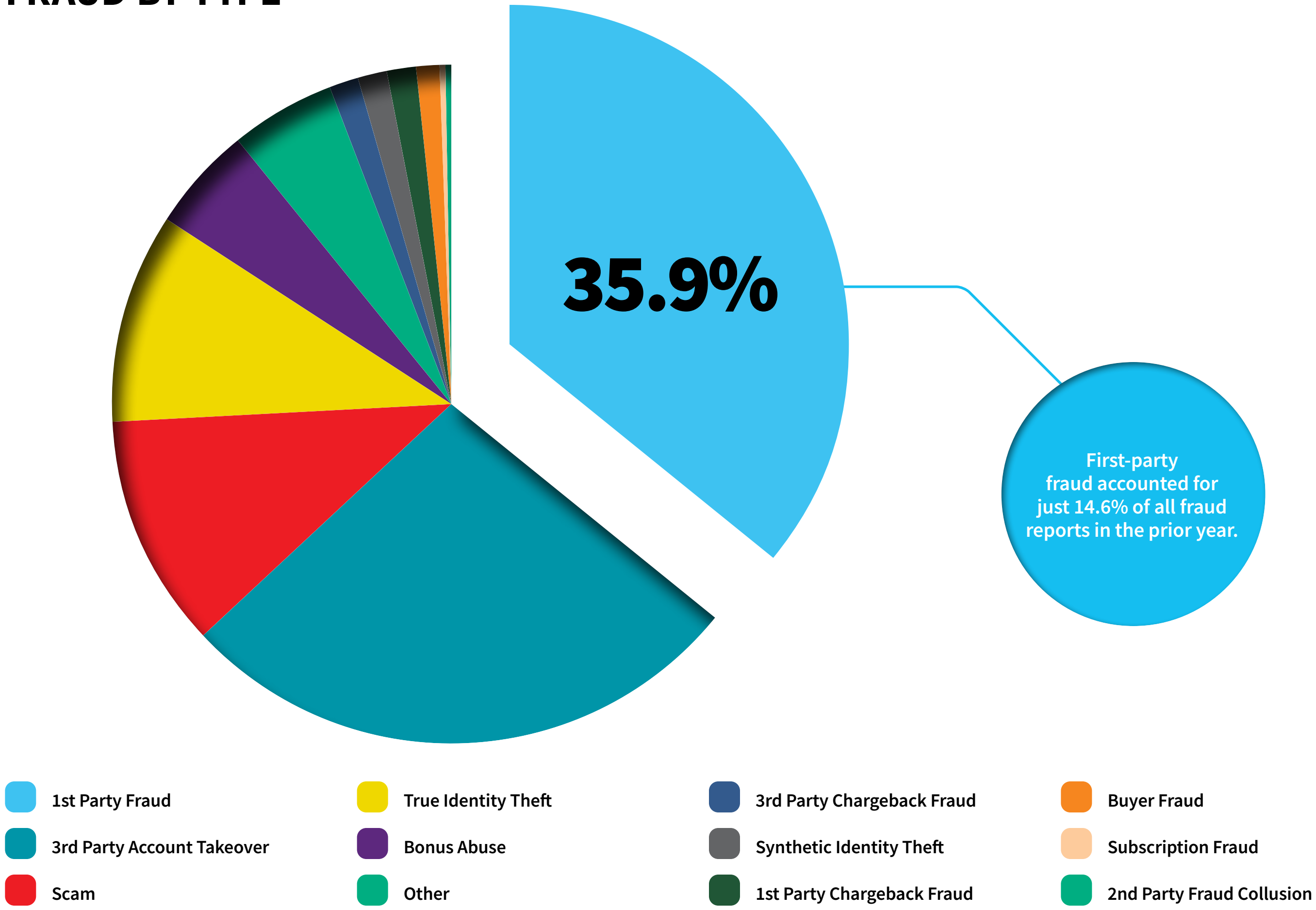
First-party fraud rises to the top of the list

The chart on this page shows how fraud attempts in Digital Identity Network are classified by our clients. The four most prevalent categories were first-party fraud, third-party account takeover, scams and true identity theft.

The threat of first-party fraud is growing globally. “Buy Now, Pay Later” (BNPL) clients reported more first-party fraud, as did financial institutions in general. Periods of inflation and the rising cost of living are known to motivate consumers to attempt first-party fraud. Increased institutional liability for scams, driven by regulation, has also raised concerns of first-party fraud if scam victims are fully reimbursed for all scam losses.

The number of clients reporting third-party account takeover cases also grew, although at a much slower pace than first-party fraud. This was particularly noticeable in Asia, where many scams were related to account takeover, as victims were led to reveal their authentication details through phishing sites. (In Asia, a client may classify such a scenario as either a scam or an account takeover.)

FRAUD BY TYPE



First-party fraud accounted for just 14.6% of all fraud reports in the prior year.

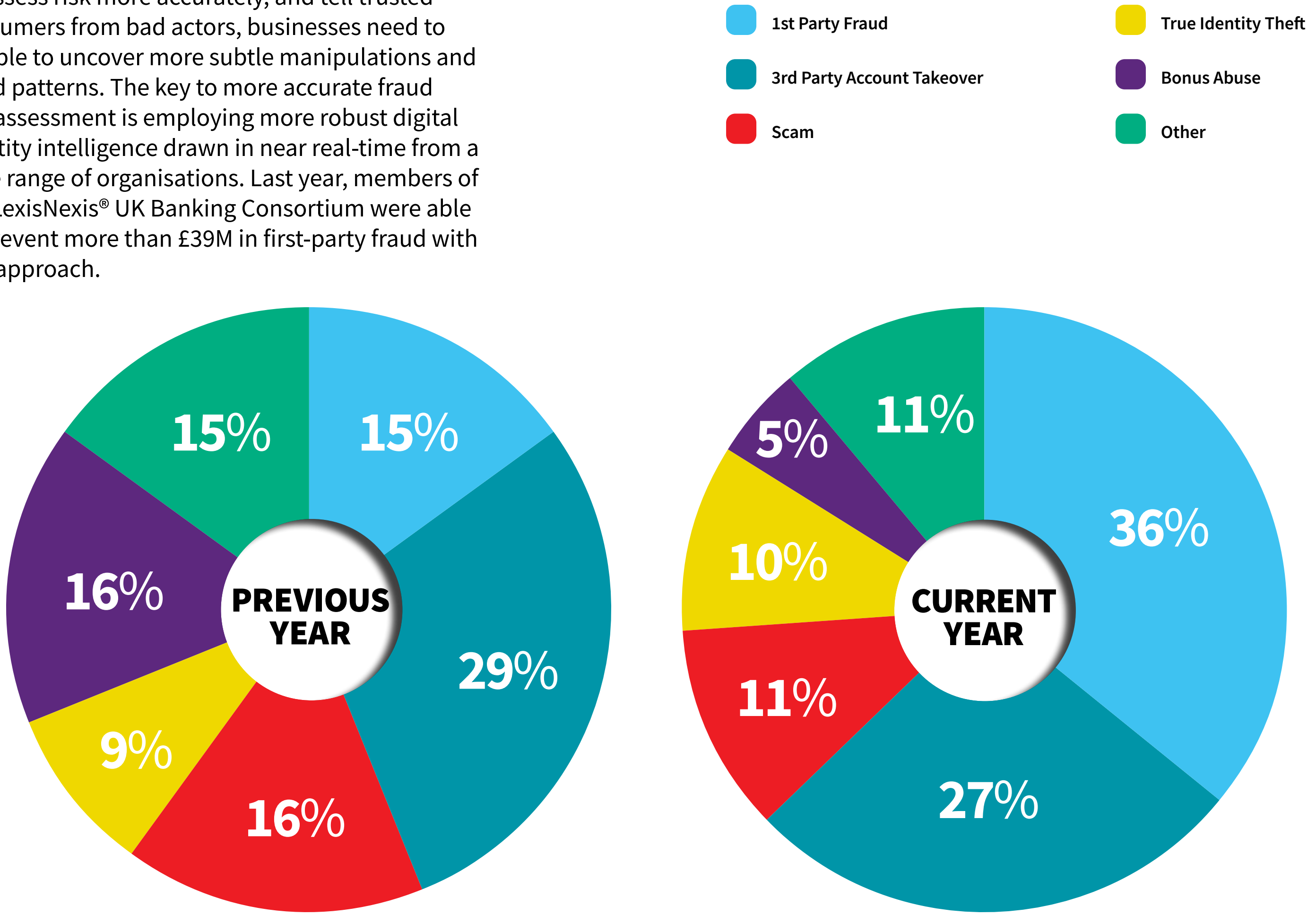
The Rising Challenge of First-Party Fraud

Consumer intent separates good risk from bad

As economic pressures build, so does the incidence of first-party fraud, as more consumers may succumb to the temptation to misuse their identities to make ends meet. First-party fraud is harder to detect than third-party fraud, since schemes such as account bust-outs and charge-back abuse involve real account-holder data (and definitions of first-party fraud still vary among organisations and industries).

Detecting first-party fraud early requires an understanding of consumer intent, to separate "good risk" from "bad risk." Distressed consumers typically apply for products and services with an intent to repay the charge, but then fail to do so. "Good risk" indicators are short-term activity that depart from the norm, such as increased interactions with payday lending businesses or credit repair address changes. "Bad risk" consumers, who never intend to repay charges, often display risky indicators repeatedly, such as VPN or proxy use, risky IP addresses, multiple names or phone numbers attached to a single digital identity, or poor reputation in the Digital Identity Network solution.

To assess risk more accurately, and tell trusted consumers from bad actors, businesses need to be able to uncover more subtle manipulations and fraud patterns. The key to more accurate fraud risk assessment is employing more robust digital identity intelligence drawn in near real-time from a wide range of organisations. Last year, members of the LexisNexis® UK Banking Consortium were able to prevent more than £39M in first-party fraud with this approach.



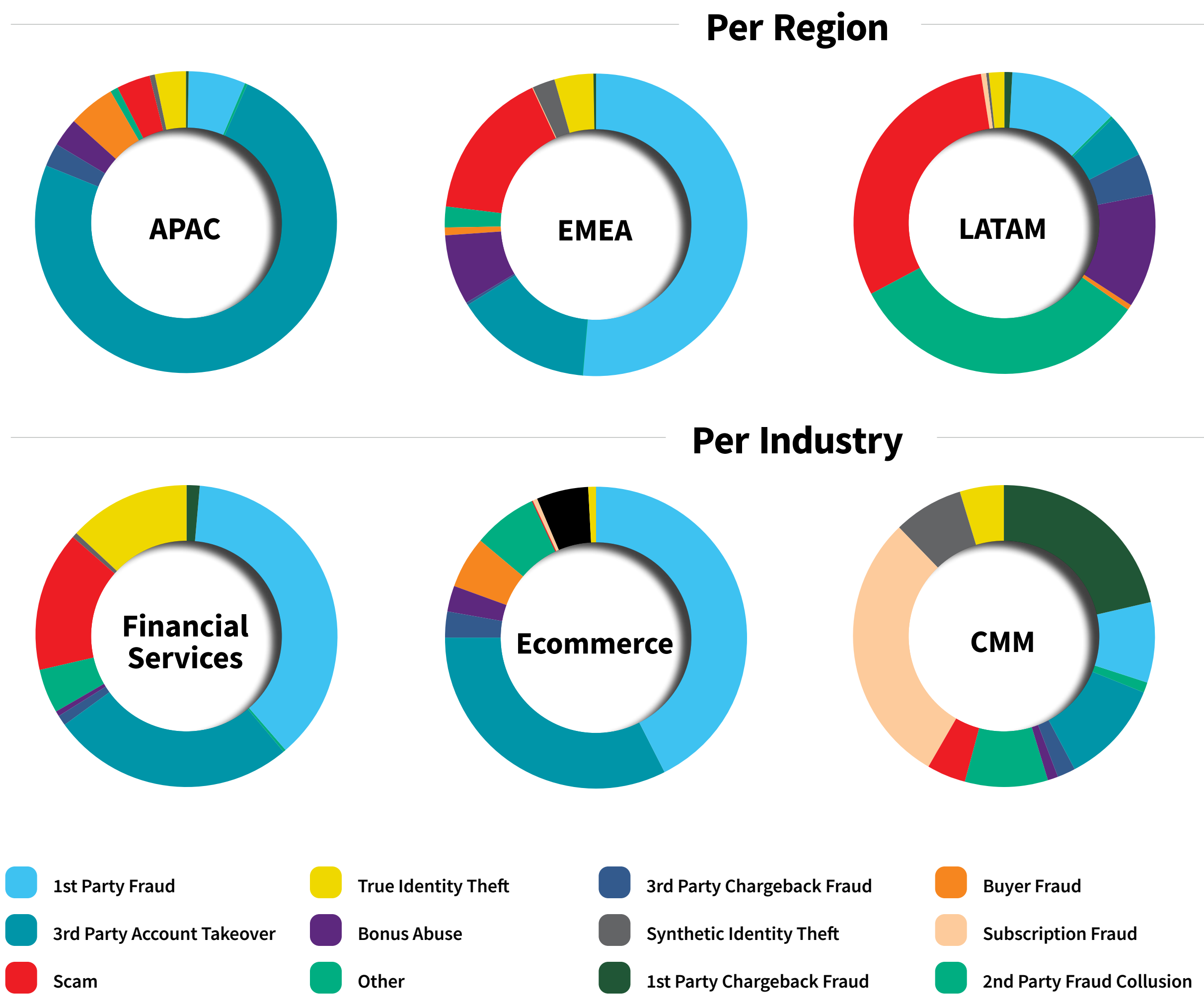
Fraud Classifications by Region and Industry

Regional fraud challenges are numerous and varied

Fraud classifications by clients around the world show clear differences driven by consumer behaviour, regulator influence, and the maturity of fraud defences and associated attack complexity.

APAC continued to see third-party account takeover (driven by phishing) as the largest concern, although mature markets were reporting a significant shift to authorised push payment scams by the end of the year. First-party fraud grew strongly as a percentage of all fraud types reported in EMEA and North America—driven by increases in both the financial services and ecommerce sectors. Identity theft is still a significant challenge in the US, while in LATAM scams were the primary concern.

In the financial services sector, third-party account takeover has decreased slightly as a percentage of reported frauds globally, enabling first-party fraud to take the top spot (as it has done also in ecommerce). Scams and true identity theft remain significant concerns, while cases of synthetic identity theft declined for ecommerce and CMM. Bonus abuse continues to be a significant problem in the gaming and gambling sector, which also saw an increase in the significance of third-party account takeover.


Per Region

Per Industry

Fraud classifications can vary between regions and industries due to combinations of local idiosyncrasies, but also nuanced differences in definitions and interpretations of fraud types.

Across the Customer Journey

Current Analysis

Each user touchpoint, from account creation to payments, can expose customers and organisations to additional risks of fraud—unless sophisticated countermeasures can address them first. Here’s what the data says.

Customer Journey Highlights

Different consumer touchpoints present different threats for frauds and scams

New Account Creation

- **1 in every 11** new account creations are attacks
- CMM and gaming and gambling have the highest industry attack rates **at 13% and 8.5% respectively**

Logins

- 0.6% attack rate (23% decline YOY)
- Ecommerce has the highest industry attack rate **at 3.4%**

Payments

- Highest mobile share of transactions **(82% of payments are mobile)**
- Most frequently attacked use case by volume

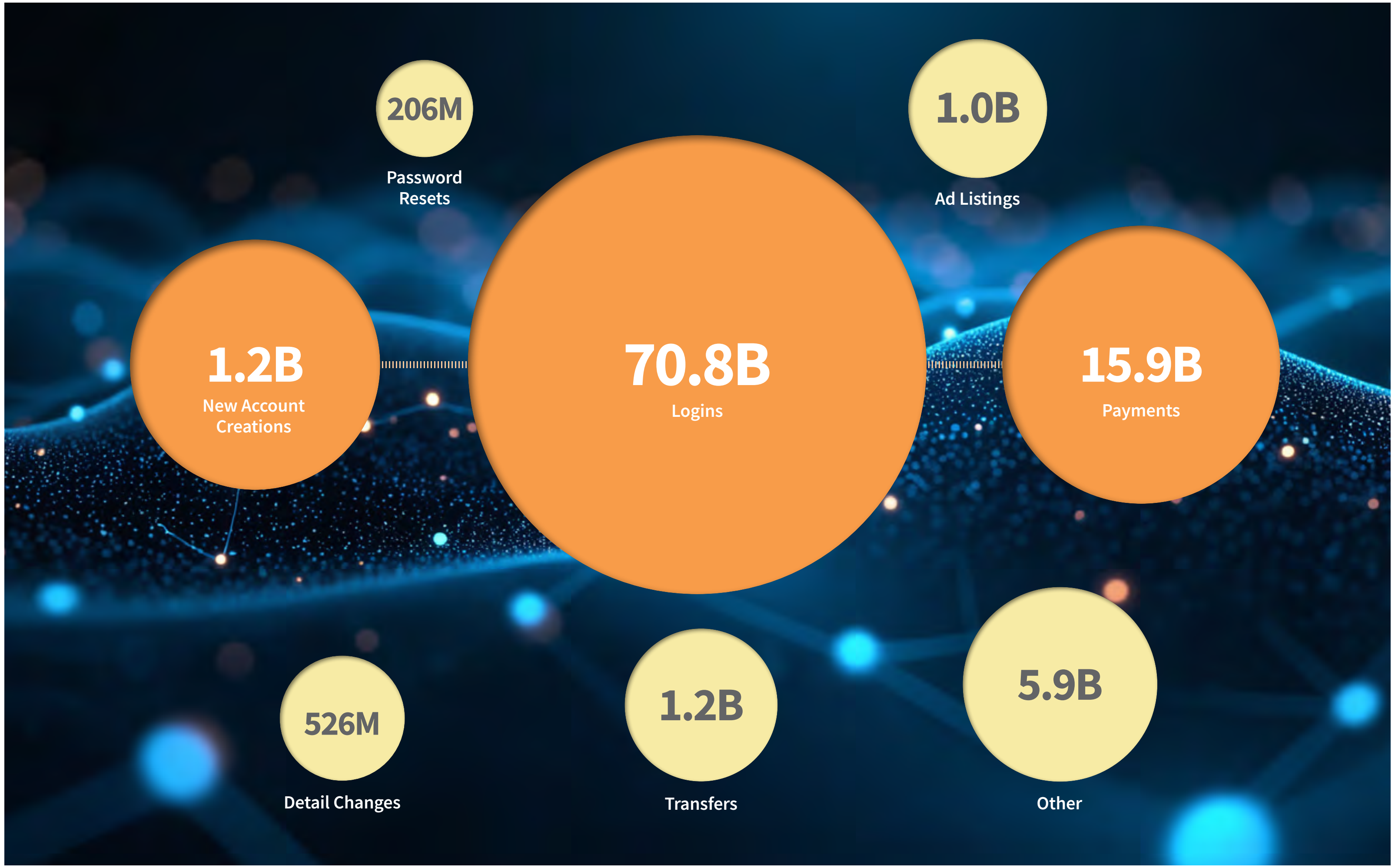
Details Change

- **92% YOY increase in attack rate**
- Vulnerability here can lead to compromise of out-of-band authentication

Volume of Transactions by Use Case Across the Online Journey

Profiling risk across each customer touchpoint

Logins provide the highest number of transactions in the user journey by far, which also present frequent security risks. But payments and new account creations together accounted for 17 billion online transactions, each of them another opportunity for fraudsters. (The "other" category, accounting for almost 6 billion transactions, includes new device registrations, digital downloads, account balances, loan acceptances, auction bids and more.)



Transaction volume by use case is calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.

Attack Risks Across Core Touchpoints

Financial app mobile sign-ups in particular are under attack

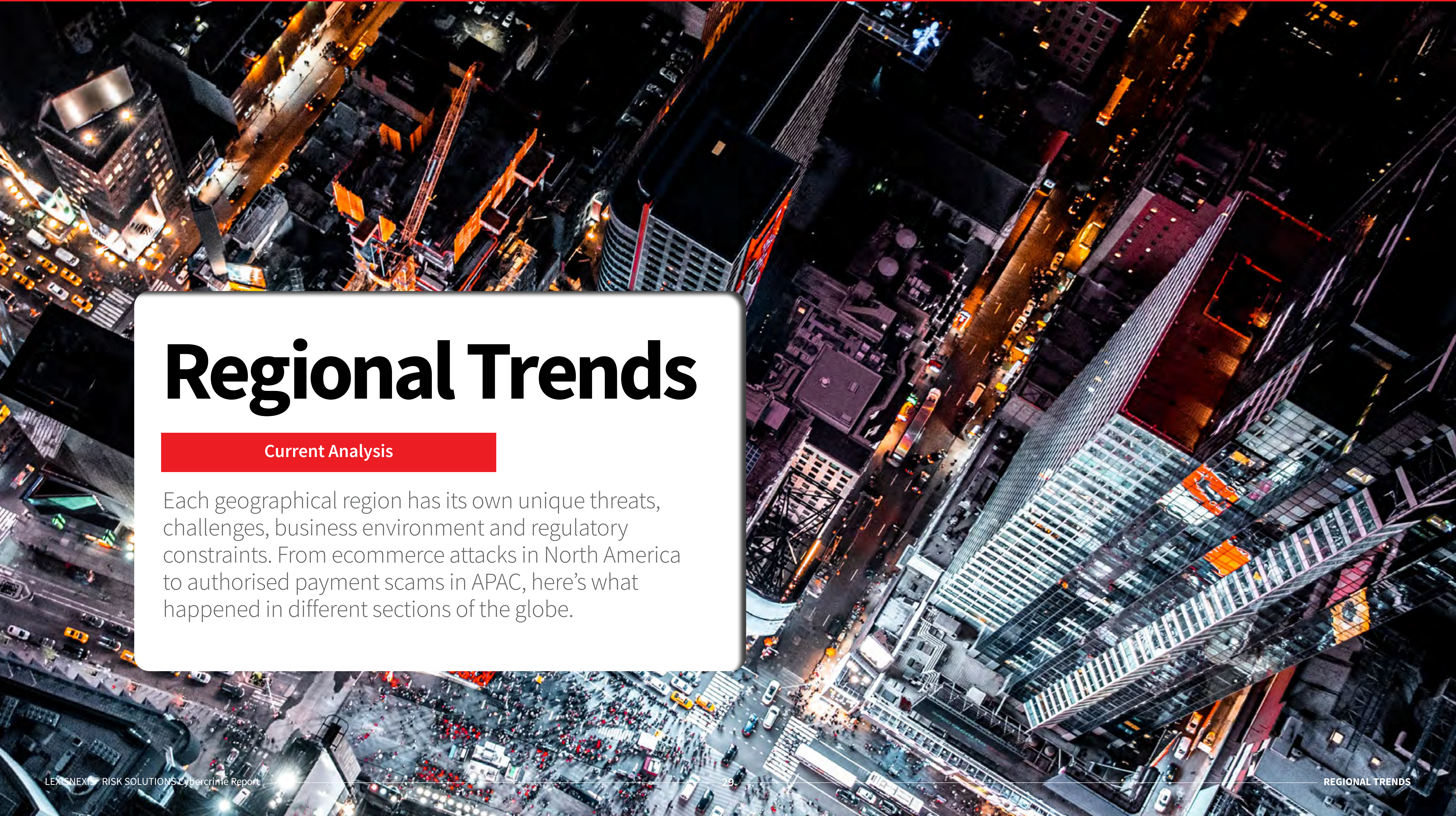
	New Account Creations	Logins	Payments
Risk Trends	While the attack rate for new account creations has remained stable YOY, this continues to be one of the highest-risk touchpoints in the entire customer lifecycle—second only to password reset risk. Sign-ups through browser channels are still significantly more risky than via mobile apps, even though the attack rate for browser channels declined YOY while the mobile app attack rate grew by 13% YOY. This is being driven by an increasing ability to sign up fully for new financial services offerings through a mobile app (the mobile app attack rate at this touchpoint, specifically for financial services, grew by 32% YOY).	After two years of significant increases in the login attack rate, the account takeover focus declined in the past year with the login attack rate dropping by 23% YOY back to 2022 levels. This decline was driven by reductions in the attack rate on both mobile channels, while the desktop attack rate remained stable. This suggests that prevention measures for mobile channel account takeover have improved. This global trend was not seen in APAC, where the login attack rate actually increased by 21% YOY (after a decline over the previous year).	Global payment attacks continued to increase in the past year, up 14% YOY after a similar increase in the prior year, with increases across all channels. EMEA was the only region which did not follow this trend, instead seeing a 15% attack rate decline YOY, with a downward trend across all industries except for Communications, Mobile and Media.
	ATTACKS		
Overall Attack Rate	⚠ 9.1%	0.6%	4.7%
Desktop Attack Rate	12.6%	1.2%	4.5%
Mobile Browser Attack Rate	9.6%	1.8%	5.4%
Mobile App Attack Rate	4.2%	0.3%	4.2%

Attack volume and attack rate by use case are calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.

Attack Risks Across Additional High-Risk Touchpoints

Account-detail-change attack risk increases, while other touchpoints are targeted less

	Password Resets	Detail Changes	Ad Listings	Transfers	Other
Risk Trends Attack volume and attack rate by use case are calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.	After significant increase two years ago (up 135% YOY), the attack rate for password resets declined by 19% YOY. It still remains a high-risk touchpoint, however, supporting the account takeover attack scenario. Attack trends continue to favour the desktop browser channel (attack rate up 16% YOY), while mobile app attack rates continue to fall with a decline of 64% YOY after a similar decline two years ago.	Last year saw another significant increase in the attack rate for details change events (up 92% YOY after an even greater increase the prior year). These attacks facilitate interception of authentication messages such as one-time passcodes by changing the account's registered phone number or email address. These attacks may occur through traditional web or mobile channels—as well as through chatbot channels, increasingly, which may be less secure against these types of attacks.	Attack rates for ad listings declined again (down 60% YOY) after declining slightly two years ago. Ad listings allow fraudsters to control the sale or promotion of goods and services, provide a way of monetising stolen goods or create phony reviews to facilitate sales.	Attack rates associated with transfers declined 39% YOY, following a downward trend already seen two years ago. Transfers move money into a different account within a customer's overall profile, an action that can precede a fraudulent payment event.	This category encompasses several other high-risk touchpoints, such as new channel registration, standing order mandates, direct debits and beneficiary modifications. Attack rates associated with these other touchpoints rose 47% YOY, after a 24% YOY increase two years ago.
	ATTACKS				
Overall Attack Rate	11.1%	7.3%	0.2%	0.4%	1.9%
Desktop Attack Rate	27.0%	12.6%	0.5%	0.7%	2.7%
Mobile Browser Attack Rate	2.3%	15.1%	0.3%	0.9%	2.6%
Mobile App Attack Rate	0.7%	1.4%	0.1%	0.4%	1.3%



Regional Trends

Current Analysis

Each geographical region has its own unique threats, challenges, business environment and regulatory constraints. From ecommerce attacks in North America to authorised payment scams in APAC, here's what happened in different sections of the globe.

Regional Highlights

APAC outpaces the rest of the world in attacks

APAC

+16% transaction volume YOY

+61% human-initiated attacks YOY

+6% bot volume YOY

EMEA

+12% transaction volume YOY

-5% human-initiated attacks YOY

-46% bot volume YOY

LATAM

+13% transaction volume YOY

-17% human-initiated attacks YOY

-9% bot volume YOY

North America

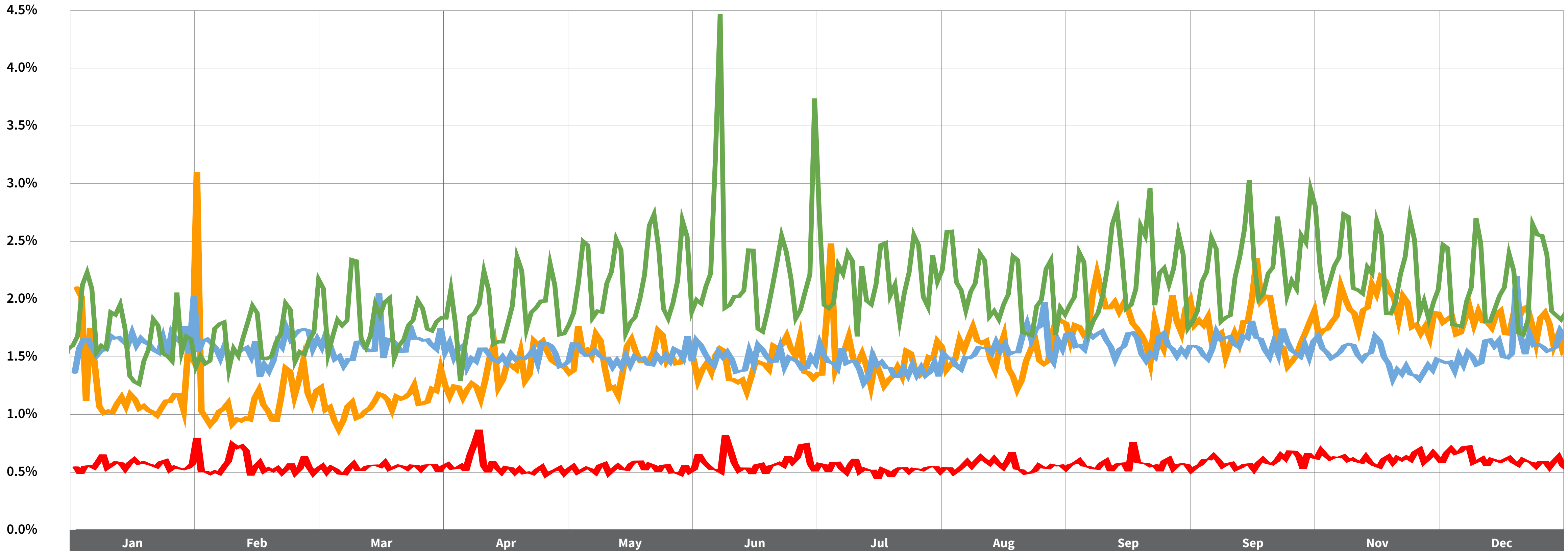
+14% transaction volume YOY

+31% human-initiated attacks YOY

0% bot volume YOY

Identity Abuse Index by Region

APAC attack rate increased beyond other regions



🟧 **APAC** reversed course from a slight decline two years ago as its attack rate grew significantly in the last 12 months.

🟥 **EMEA** continues to see the lowest regional attack rate across the regions.

🟦 **LATAM** has seen a sustained decrease in its attack rate which started towards the end of the prior year, now putting it lower than that of North America.

🟩 **North America** again saw attack rate growth in both the United States and Canada as ecommerce continues to be targeted.

APAC Transaction and Attack Patterns

Human-initiated attacks are exploding in the region

Attack Spotlights

- Multiple mobile banking app login attacks originated from within China.
- Streaming services in the region came under attack from Australia, India, Taiwan and Singapore.

TRANSACTIONS

TRANSACTIONS PROCESSED

VOLUME	CHANGE YOY
9.8B	+16%

TRANSACTIONS BY CHANNEL

Mobile	Desktop
86%	14%

Mobile App	Mobile Browser
87%	13%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

VOLUME	CHANGE YOY
143M	+61%

AUTOMATED BOT ATTACK VOLUME

VOLUME	CHANGE YOY
423M	+6%

TRANSACTIONS BY CHANNEL

Mobile 50%

Desktop 50%

Change YOY in attacks coming from mobile devices -7%

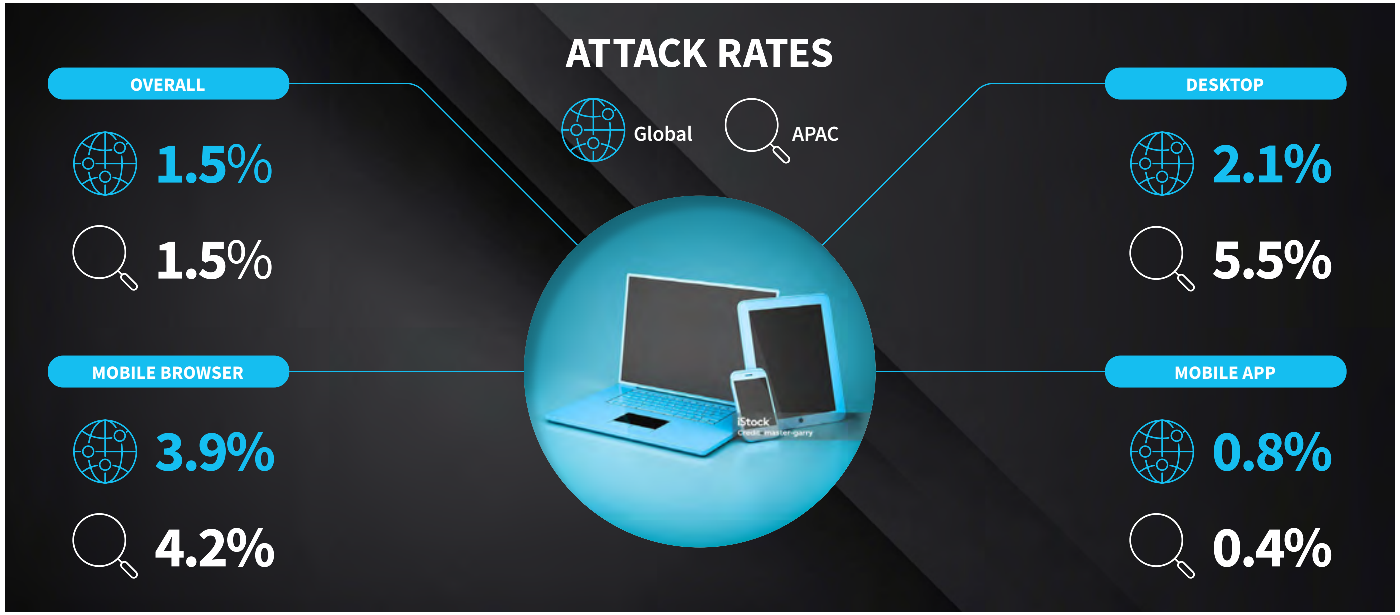
APAC’s Position vs. Global Figures

Scams rage across the region as authorised fraud begins to dominate

The attack rate in APAC grew by 37% YOY to reach 1.5%—backed up by police, central bank and media reports in the region that stated losses from scams and other types of digital fraud did not slow down. In fact, many countries in the region reported record fraud losses last year.

While the spotlight remains focused on cases that involved unauthorised fraud, such as credit card fraud and phishing attacks, the largest financial losses were frequently connected to authorised payment scams. Cybercriminals used a variety of social engineering tactics to target their victims, including impersonation and deepfakes. Several recent examples of the ever-expanding scam industry showed this problem was actually escalating in some parts of APAC rather than being contained:

- **Japan, a country that initially appeared to be insulated from the rest of APAC when it came to scams, reported record-high losses involving romance and investment scams and phone-related social engineering scams. This is mirrored in the attack rate measured for Japan last year, up 62% YOY at 3.2%.**
- **Hong Kong was at the top of per-capita fraud losses.**



ATTACK RATES

🌐 Global   🔍 APAC

OVERALL

🌐 1.5%

🔍 1.5%

DESKTOP

🌐 2.1%

🔍 5.5%

MOBILE BROWSER

🌐 3.9%

🔍 4.2%

MOBILE APP

🌐 0.8%

🔍 0.4%

- **In Singapore, 86% of scams reported to the police involved self-effected activities, also known as authorised payment scams. This form of attack was the most common fraud classification from Singapore clients using the Digital Identity Network solution last year.**

The scam industry in APAC continues to grow and is reported to employ hundreds of thousands of people—some of them working as forced labour. There has been movement by authorities in some countries to clamp down on these scam centres in recent months.

Fraud Links Across APAC

The Digital Identity Network solution spots fraud attempts as they happen

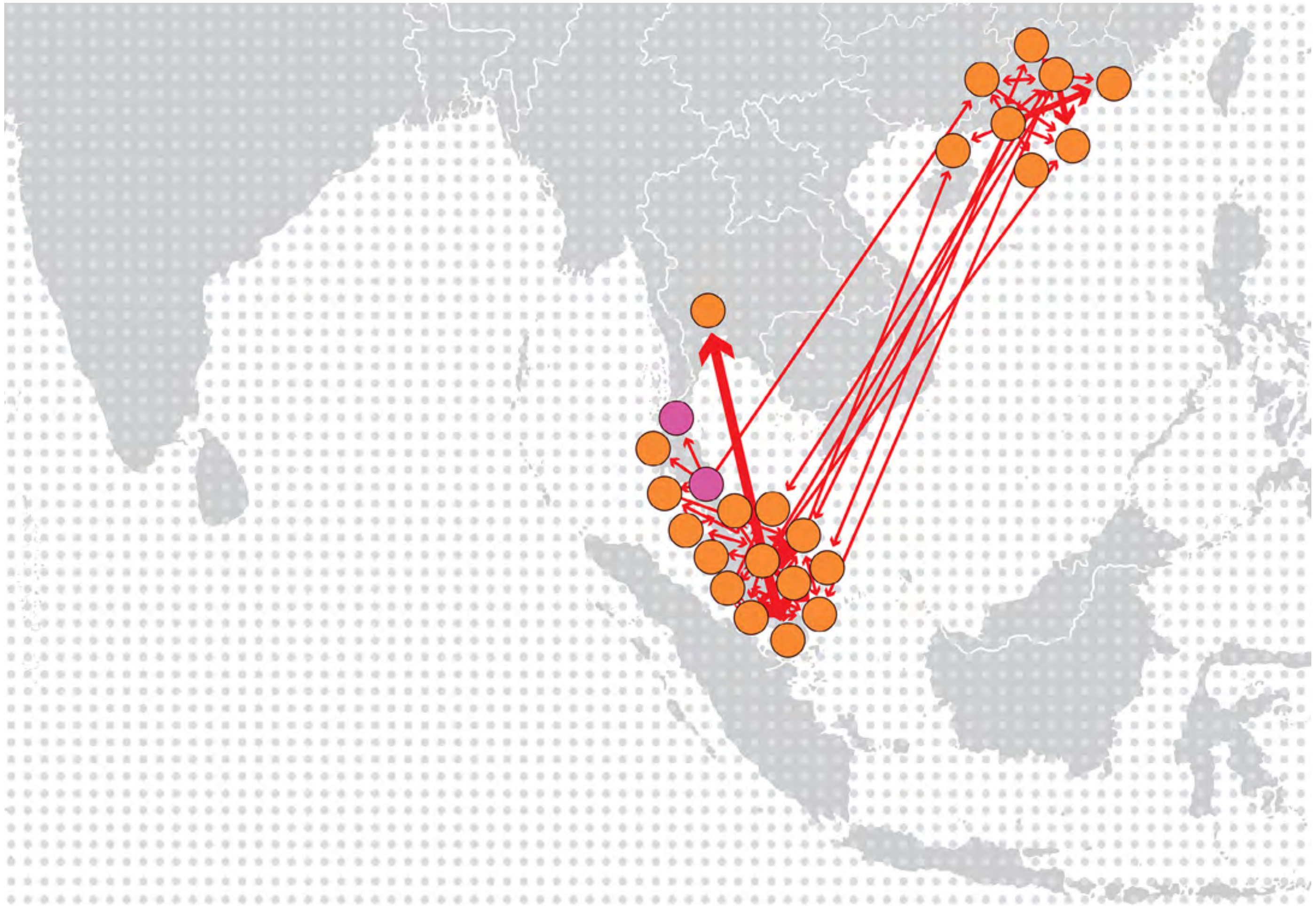
This illustration shows fraud (linked by digital identity) connected to organisations operating in APAC during the last quarter of last year.

Each circle represents an individual organisation, while each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation crossing over to another organisation within Digital Identity Network. A thicker line denotes a higher volume of attacks.

This view showcases both the interconnected nature of fraud rings within financial institutions at the country level, but also the increased cross-border nature of fraud, encouraged by the expansion of instant payment frameworks' interoperability across the region.

● Financial Service

● Digital Wallet



Locations have been changed to anonymise the institutions involved.

EMEA Transaction and Attack Patterns

Attacks via mobile channels jump

Attack Spotlights

- Account takeover attacks on Gaming operators from the US spiked in May.
- Password reset attacks on marketplaces increased in the second half of the year from Russia, the Netherlands and Poland in particular, as well as many other countries.

TRANSACTIONS

TRANSACTIONS PROCESSED

VOLUME 31.8B

CHANGE YOY +12%

TRANSACTIONS BY CHANNEL

Mobile 86%

Desktop 14%

Mobile App 82%

Mobile Browser 18%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

VOLUME 172M

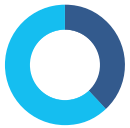
CHANGE YOY -5%

AUTOMATED BOT ATTACK VOLUME

622M

-46%

ATTACKS BY CHANNEL



Mobile 62%

Desktop 38%

Change YOY in attacks coming from mobile devices +16%

EMEA's Position vs. Global Figures

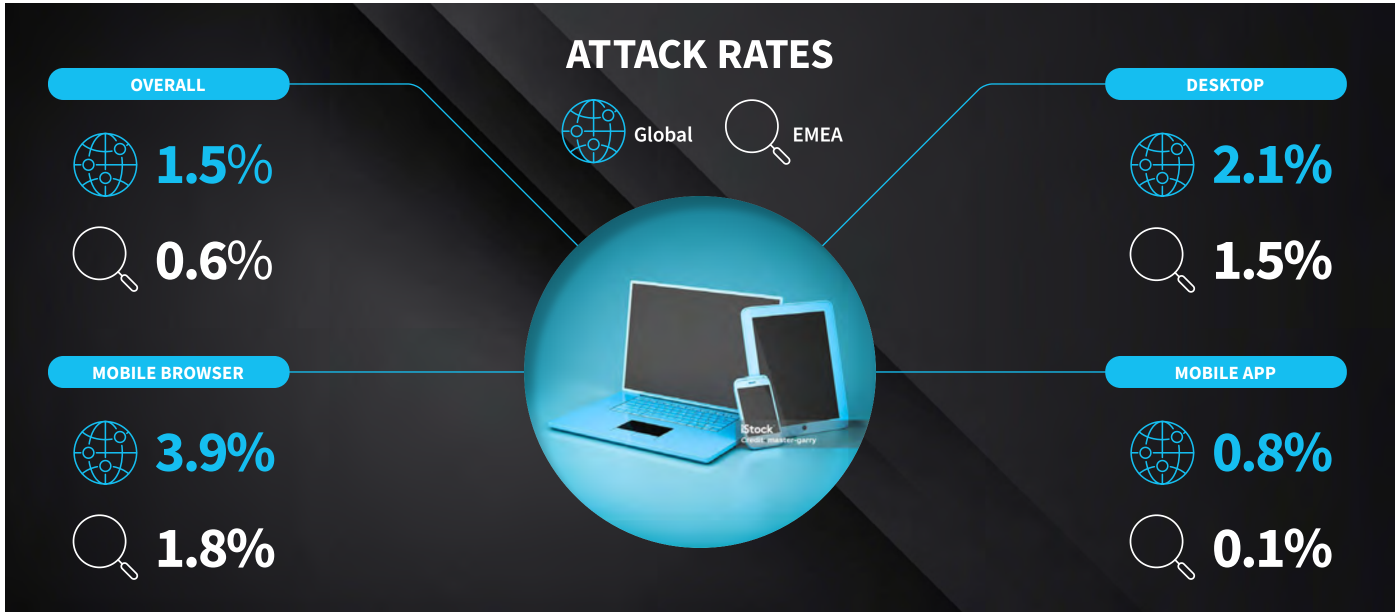
The region faces evolving scams and tightening regulations

EMEA saw a reduced attack rate of 0.6% last year (down 19% YOY), reconfirming its position as the region with the lowest attack rate and most mature fraud prevention landscape.

This attack rate decline was driven by reduced fraud attacks in ecommerce specifically—however, as discussed on page 18 ("Making the 3D Secure Journey Smarter and Safer"), there are now clear examples of fraudsters refocusing their attention on ecommerce with scams to circumvent strong customer authentication measures introduced in recent years.

Indeed, as scam detection and prevention models in the financial services sector become more widespread, fraudsters are looking to exploit the same techniques across other industries such as ecommerce, travel and telecommunications.

The effects of regulatory changes (UK Payment Systems Regulator liability definitions went live in October 2024 and Europe awaits finalisation of PSD3) will be seen over the coming months.



ATTACK RATES

Global EMEA

OVERALL
1.5%
0.6%

DESKTOP
2.1%
1.5%

MOBILE BROWSER
3.9%
1.8%

MOBILE APP
0.8%
0.1%

Fraud Links Across EMEA

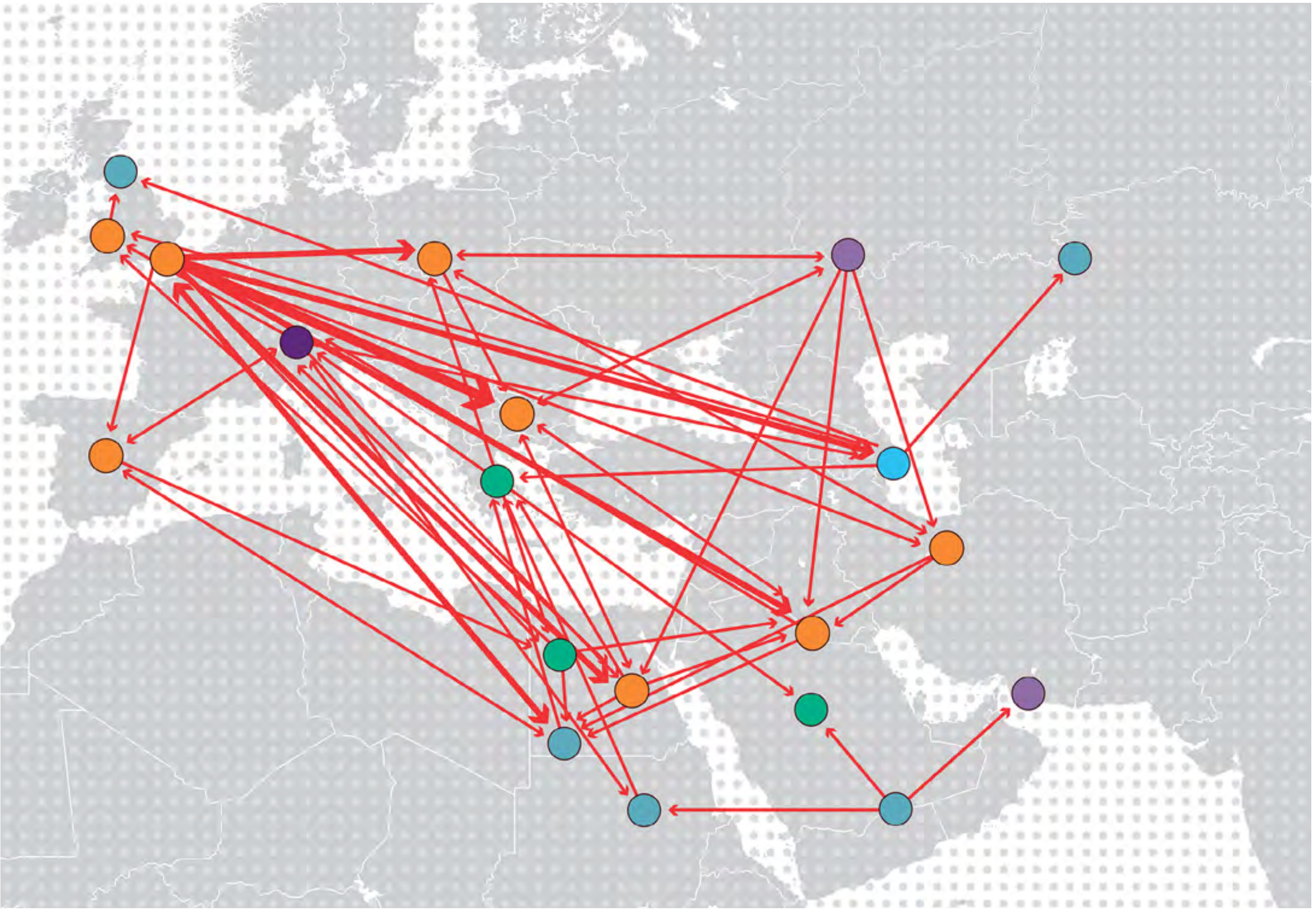
The Digital Identity Network solution spots fraud attempts as they happen

This illustration shows fraud (linked by digital identity) connected to organisations operating in EMEA during the last quarter of last year.

Each circle represents an individual organisation. Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation within Digital Identity Network. A thicker line denotes a higher volume of attacks.

This view showcases both the interconnected nature of fraud rings across traditional sectors such as finance, telecom and ecommerce, but also the re-emergence of travel fraud following several years of subdued volumes due to Covid.

- ● Financial Service
- ● Retailer
- ● Marketplace
- ● Buy Now Pay Later
- ● Telco
- ● Travel



Locations have been changed to anonymise the institutions involved.

LATAM Transaction and Attack Patterns

Mobile attacks against client organisations fell in this mobile-dominated region

Attack Spotlights

- Periods of increased login attacks on banking and ecommerce mobile apps originating from Argentina and Brazil.
- Media streaming account creation attacks originating from Colombia in December.

TRANSACTIONS

TRANSACTIONS PROCESSED

	VOLUME	CHANGE YOY
	15.5B	+13%

TRANSACTIONS BY CHANNEL

Mobile	Desktop
92%	8%

Mobile App	Mobile Browser
93%	7%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

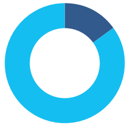
	VOLUME	CHANGE YOY
	237M	-17%

AUTOMATED BOT ATTACK VOLUME

	VOLUME	CHANGE YOY
	343M	-9%

ATTACKS BY CHANNEL

Mobile 85%



Desktop 15%

Change YOY in attacks coming from mobile devices -4%

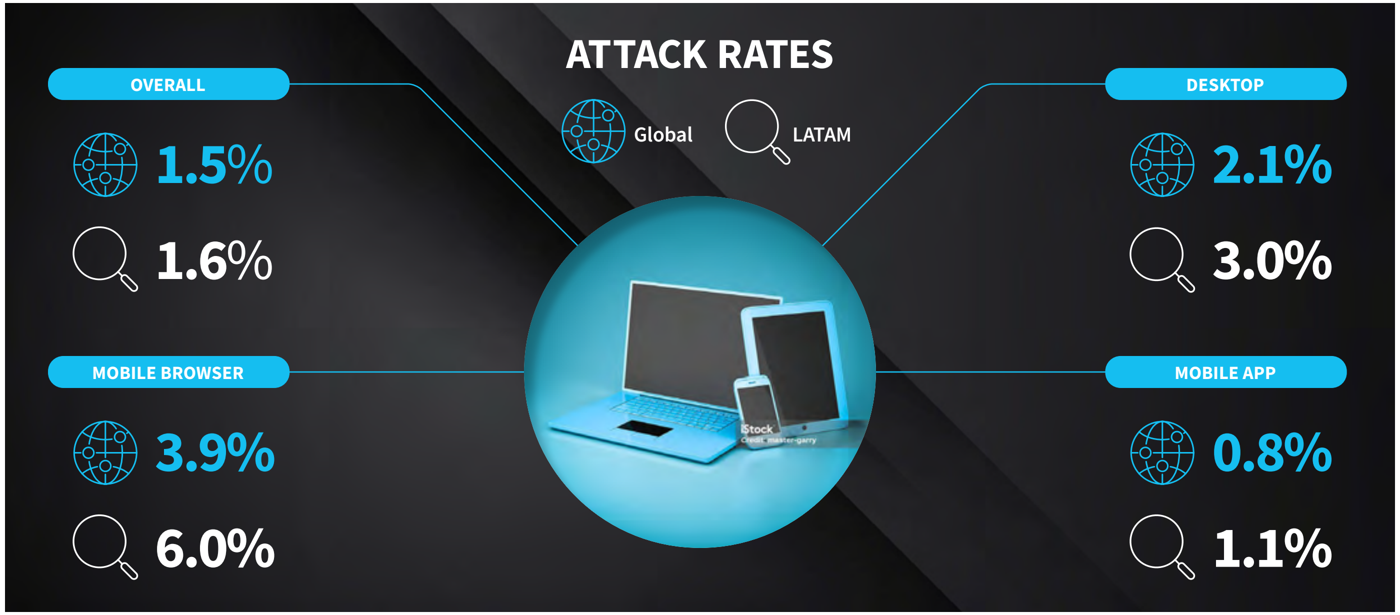
LATAM’s Position vs. Global Figures

Attack rate approaches global average, but gaming and gambling sector is targeted

Reports of fraud cases continue to rise in many parts of the region, but this stands in contrast to the attack rate seen in the Digital Identity Network solution, which actually decreased significantly last year (down 27% YOY), after also declining the prior year. The LATAM attack rate at 1.6% is still slightly higher than the global average, and reflects the fact that fraud is prevalent, especially as the rapid adoption of digital services across the region has tended to outpace security infrastructure (governments are encouraging the digitalisation of public services and driving financial inclusion).

The data suggests that fraudsters are starting to avoid targeting organisations that use modern fraud prevention solutions, and are instead attacking enterprises who have not yet put layered fraud prevention systems in place. The drop in attack rate on the mobile app channel last year (down 39% YOY) was particularly striking.

Instant payment schemes continue to dominate the region, with the well established PIX payments in Brazil and somewhat less successful CoDi in Mexico in 2025 joined by a similar scheme (Bre-B) in Colombia. As anticipated in last year’s Cybercrime Report, the emerging gaming and gambling sector saw significant growth in the attack rate in the region, up 55% YOY.



ATTACK RATES

Global LATAM

OVERALL
1.5%
1.6%

DESKTOP
2.1%
3.0%

MOBILE BROWSER
3.9%
6.0%

MOBILE APP
0.8%
1.1%

Fraud Links Across LATAM

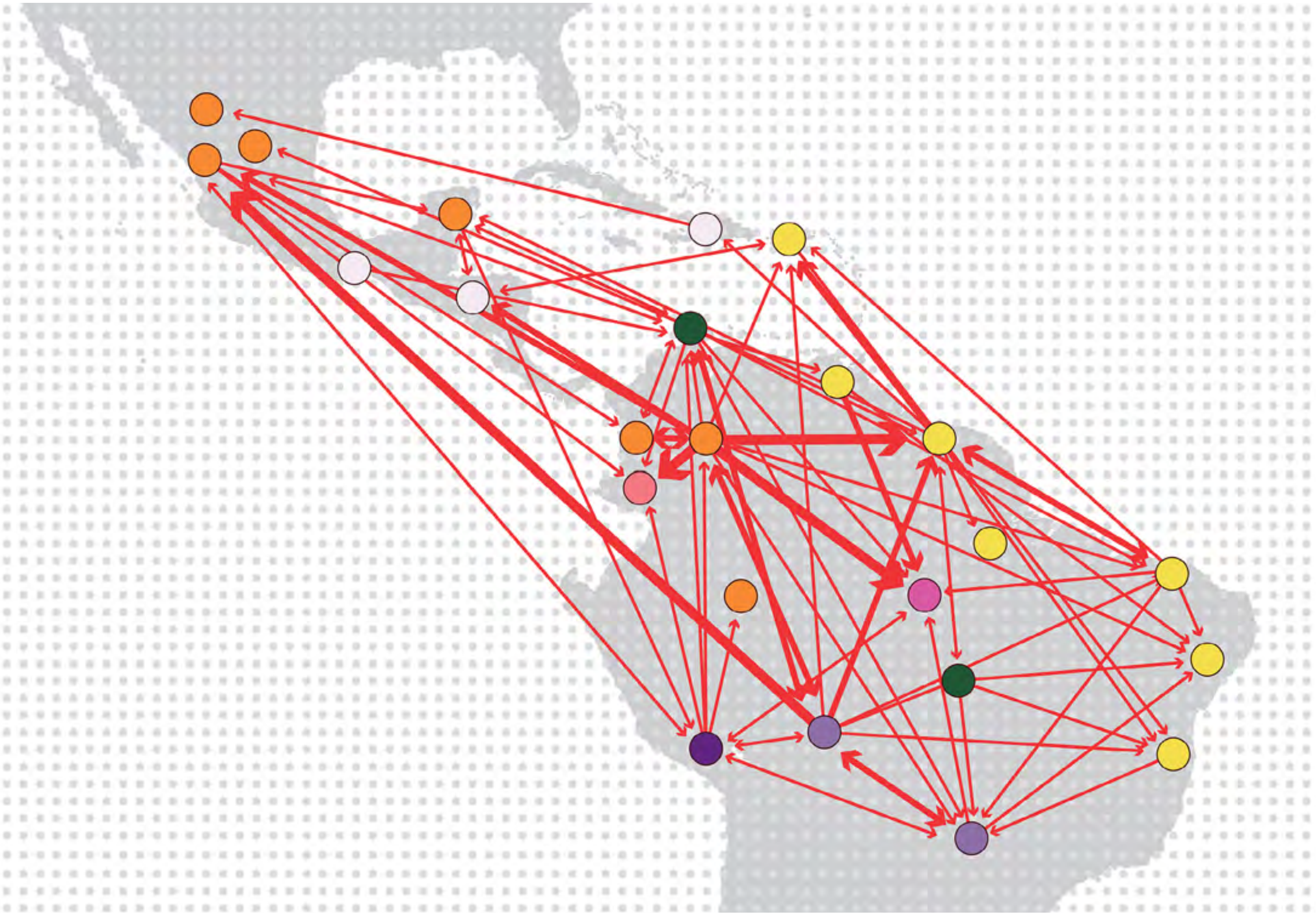
The Digital Identity Network solution spots fraud attempts as they happen

This illustration shows fraud (linked by digital identity) connected to organisations operating in Latin America during the last quarter of last year.

Each circle represents an individual organisation. Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation within Digital Identity Network. A thicker line denotes a higher volume of attacks.

This view showcases both the growth of fraud in the digital gaming and gambling sector in the region and shows the crossover of fraud networks into financial services and ecommerce.

- ● Financial Service
- ● Digital Bank
- ● Gaming and Gambling
- ● Retailer
- ● Loyalty Program
- ● Insurance
- ● Travel
- ● Digital Wallet



Locations have been changed to anonymise the institutions involved.

North America Transaction and Attack Patterns

Bots hold steady as human-initiated attacks increase

Attack Spotlights

- Attacks from various European countries on North American mobile banking apps took place in January and May.
- Continued rise in domestic account takeover attacks on US ecommerce sites.

TRANSACTIONS

TRANSACTIONS PROCESSED

VOLUME 43.7B

CHANGE YOY +14%

TRANSACTIONS BY CHANNEL

Mobile 71%

Desktop 29%

Mobile App 76%

Mobile Browser 24%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

VOLUME 905M

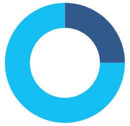
CHANGE YOY +31%

AUTOMATED BOT ATTACK VOLUME

1.7B

0%

ATTACKS BY CHANNEL



Mobile 75%

Desktop 25%

Change YOY in attacks coming from mobile devices +3%

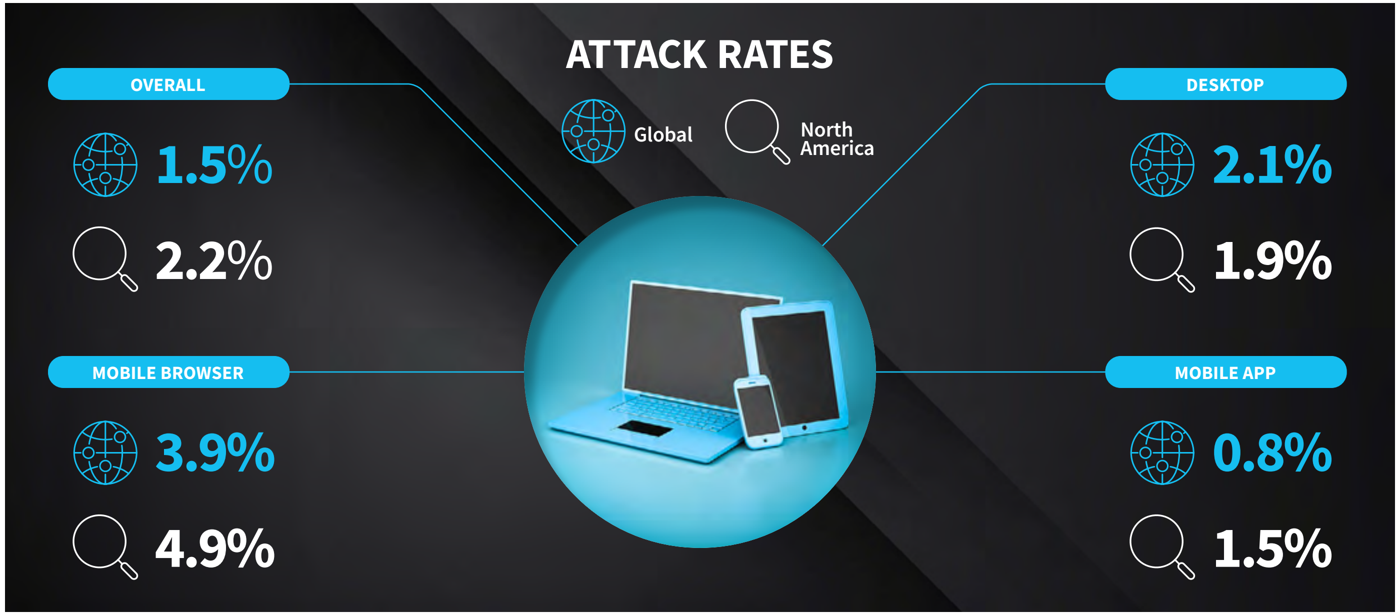
North America’s Position vs. Global Figures

Attack trends shifting to mobile drives the region’s attack rate higher

The good news is that consumer transactions in North America grew last year, with a 14% increase YOY. The bad news? The attack rate also grew, by 16% YoY, driven by a surge in attacks by people.

Mobile channels constitute 71% of total transactions, driven by mobile apps and mobile browsers. The mobile channel also continues to be a more attractive target for fraudsters: We saw a higher attack rate growth on mobile apps than web browsers (even if the mobile app attack rate at 1.5% continues to be the lowest across channels). North America also maintains a higher attack rate overall and on mobile apps compared to global attack rates.

Banks, retailers and other businesses continue to adopt a multi-layered approach to fraud detection across different channels and use cases. This increasingly goes beyond onboarding, logins and payments, expanding to include password resets, details change and other touchpoints, continuing to secure the full customer journey. Businesses in the region are increasingly incorporating behavioural biometrics as a key component in their fraud prevention strategy to effectively fight fraud.



ATTACK RATES

	Global	North America
OVERALL	1.5%	2.2%
DESKTOP	2.1%	1.9%
MOBILE BROWSER	3.9%	4.9%
MOBILE APP	0.8%	1.5%

Fraud Links Across North America

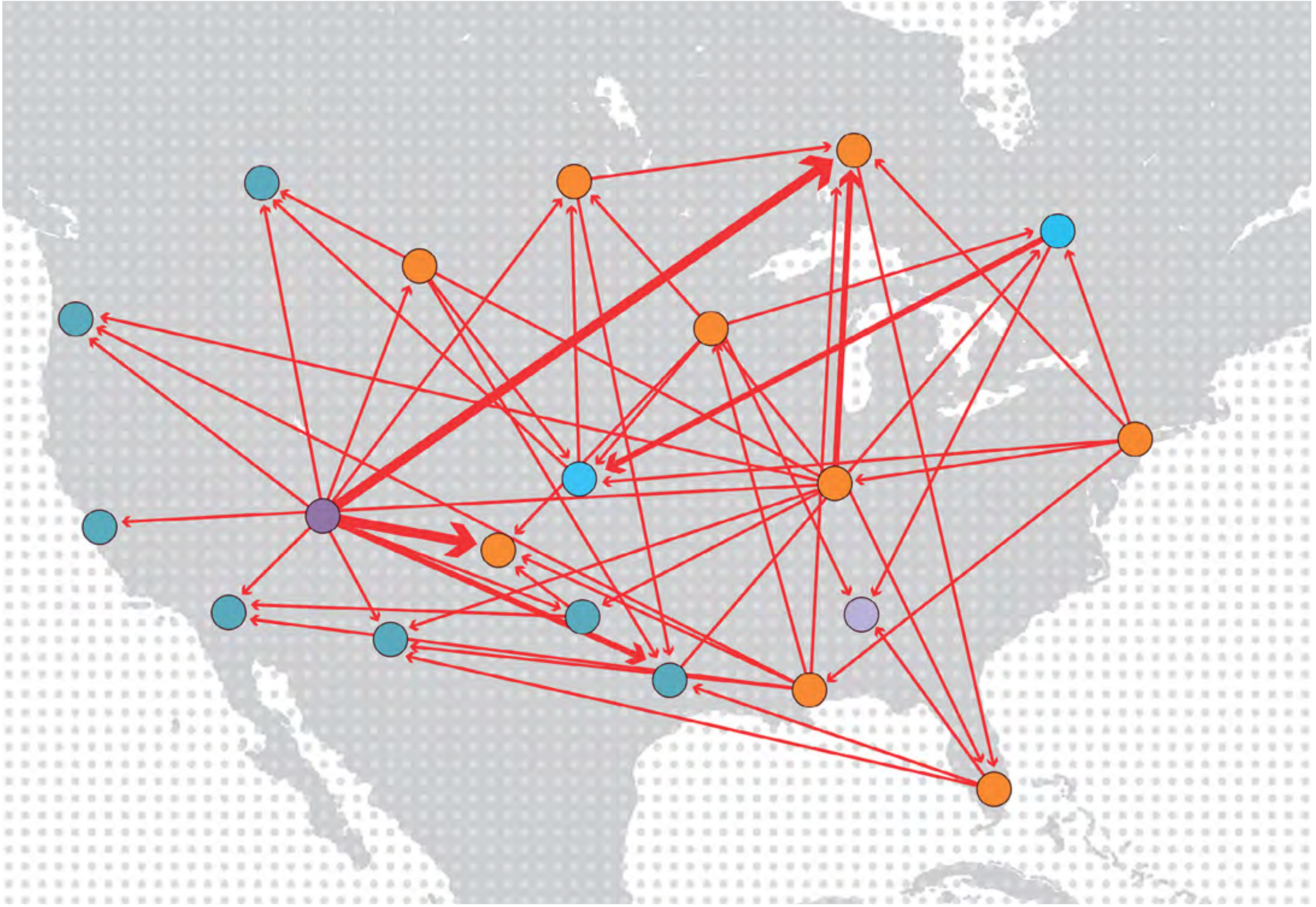
The Digital Identity Network solution spots fraud attempts as they happen

This illustration shows fraud (linked by digital identity) connected to organisations operating in North America during the last quarter of last year.

Each circle represents an individual organisation. Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation within Digital Identity Network. A thicker line denotes a higher volume of attacks.

This view showcases the tight interaction of fraud networks across marketplaces, telecom operators and the financial and payments industry. Exploring relationships in detail, a pattern is seen of fraudsters creating multiple accounts at telco operators before using these to carry out attacks at the banks. On average, three different telco accounts are linked to each of these fraudulent digital identities.

A second pattern is also revealed in the network, where fraudulent attempts at details changes at banks is then followed in 67% of cases with fraudulent payment attempts at retailers. In this scenario, fraudsters are likely changing email or phone numbers to bypass authentication challenges at the moment of purchase.



Locations have been changed to anonymise the institutions involved.

● Financial Service ● Media Streaming ● Marketplace

● Telco ● Retailer

Industry Opportunities

Current Analysis

Different industries faced very different threats, from new account fraud in communications, mobile and media to account takeover attacks in the financial services sector. Although most industries saw attack levels stabilise, they also didn't drop from their already high levels.

All-Industry Overview: Trends and Attack Patterns

Communications, mobile and media is the riskiest industry once again

Risk Trends	All-Industry Summary	Financial Services	Ecommerce	Communications, Mobile and Media	Gaming and Gambling
	With the overall human-initiated attack rate remaining stable (increasing only 1% YOY), industry level attack rates also remained stable, with the exception of CMM rising significantly.	As a highly regulated industry, generally with significant layers of fraud defences in place, financial services saw a lower attack rate (1.2%) than most other industries, although successful attacks can have greater financial impact.	Following a significant rise in attack rate last year (up 59%), the ecommerce attack rate has remained stable YOY at this higher rate of 2.8%.	The CMM attack rate was reconfirmed as the highest (5.5%) across industries last year, as it grew by 15% YOY.	The gaming and gambling attack rate at 1.0% is only slightly lower (9%) than last year.
	ATTACK RATE				
Overall Attack Rate	1.5%	1.2%	2.8%	5.5%	1.0%
Desktop Attack Rate	2.1%	1.6%	4.2%	3.7%	1.1%
Mobile Attack Rate	1.4%	1.2%	2.3%	6.3%	0.9%

Attack volume and attack rate are calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.

Financial Services Trends and Attack Patterns

Risks are increasing in payment and digital app onboarding

Financial services transactions grew strongly again last year, up 16% YOY. The APAC region saw the largest increase at 21%, as digital transformation and financial inclusion continued to expand across growth countries in the region.

The attack rate was mostly stable last year (a 3% increase YOY) after seeing several years of strong increases. This slight attack growth was driven by more attacks in North America and Asia Pacific.

Account takeover attempts were an elevated focus in both North America and APAC. The password reset attack rate in North America ballooned 90% to 2.7%, and in APAC it rose 66% to 1.3%, as fraud-sters attempted to gain access to existing accounts in these regions. The password reset attack rate in EMEA kept declining (down 70% to 0.8%) as authorised scams continue to be the attack of choice, with no need for account access.

Globally, financial services bot traffic was up 18%, while North American financial services bot traffic was up 22%.

	New Account Creations	Logins	Payments
Risk Trends	The new account creation attack rate fell by 15% YOY, driven by decreases in both desktop and mobile browsers. The mobile app attack rate, by contrast, grew 32% YOY. As more banks offer a fully digital onboarding service through the mobile app channel, this will become a key target for fraudsters.	Login attacks via mobile browsers increased, with the attack rate growing 49% YOY to reach 1.1%, overtaking the desktop attack rate for the first time. The overall login attack rate was down 23% YOY.	The ultimate high-risk event for financial services organisations, the payment attack rate increased again by 9% YOY, implying an increased financial risk for banks. Attack growth occurred most on the desktop channel.
ATTACK RATE			
Overall	7.1%	0.4%	6.1%
Desktop	9.2%	0.8%	5.6%
Mobile Browser	8.4%	1.1%	6.9%
Mobile App	4.4%	0.3%	5.6%

Ecommerce Trends and Attack Patterns

Existing customer accounts see continued abuse

The ecommerce attack rate remained stable but elevated last year, after climbing 59%. Ecommerce transaction growth was essentially flat YOY, as was attack volume growth. As discussed elsewhere in this report, ecommerce fraud can take various forms and varies regionally, being impacted by regulations (such as PSD2) as well as consumer preference (such as popularity of credit cards or BNPL). Scams related to ecommerce payments are also being reported more frequently.

One notable increase was significant growth in the attack rate (up 78% YOY) on details change events, where fraudsters try to take over existing accounts by replacing the existing email address, phone number or delivery address linked to the account with the fraudster's details. This can also compromise the authentication layer, which validates that the customer is really the one making a purchase, by redirecting one-time passcodes to the fraudster's email or phone. This increasing trend has been seen for several years, but has accelerated rapidly in the past two years.

	New Account Creations	Logins	Payments
Risk Trends	We saw little change in the general high risk of new account creations for ecommerce, with the attack rate up slightly (2% YOY). This growth was driven by attacks on the mobile channel.	After the attack rate for logins doubled two years ago, it remained at this elevated level last year. Account takeover attempts are being supported by elevated attacks on the "change of personal details" options on websites and apps.	The payment attack rate for ecommerce increased by 8% YOY, driven by an increase in mobile app payment attacks, with the mobile app attack rate growing by 34%.
ATTACK RATE			
Overall	7.5%	3.4%	2.6%
Desktop	14.6%	3.4%	3.4%
Mobile Browser	5.0%	5.2%	2.7%
Mobile App	3.5%	1.3%	2.2%

Communications, Mobile and Media Trends and Attack Patterns

The attack rate keeps increasing in an already high-risk industry

The only industry to see significant attack rate growth last year was communications, mobile and media (CMM), up 15% YOY, continuing an upward trend that started two years ago.

As diversification in the industry continues to drive more digital service offerings around the world, attacks that focus on creating fraudulent new accounts for these services also continue to increase.

Another reason for the prevalence of new account fraud in CMM is that phone numbers are becoming an increasingly dominant identity authentication or verification factor in other industries. Fraudulent new phone numbers are used to create accounts in industries such as ecommerce, gaming and gambling, financial services and mobile money. This problem is especially prevalent in APAC, LATAM and Africa, where a phone number is generally the leading identity factor.

The attack rate at new account creation was up 8% YOY to 13.2%, while the attack rate at both login (0.7%) and payment (3.1%) were down significantly (-31% and -26% YOY respectively). Much of the attack rate increase was seen specifically in the APAC region, where telecom operators are coming under increasing pressure from regulators to play a greater role in preventing fraud and scams.

	New Account Creations	Logins	Payments
Risk Trends	After decreasing two years ago, the new account creation attack rate for CMM increased by 8% YOY last year, returning to levels seen in 2021 and 2022.	The login attack rate decreased significantly (down 31% YOY), although elevated attacks were seen on the "change of personal details" options on websites and apps, similar to what was observed in ecommerce.	After doubling two years, the payment attack rate decreased by 26% YOY.
ATTACK RATE			
Overall	⚠ 13.2%	0.7%	3.1%
Desktop	💻 20.7%	0.4%	5.2%
Mobile Browser	📱 12.0%	1.0%	4.3%
Mobile App	▢ 8.9%	0.1%	2.5%

Gaming and Gambling Trends and Attack Patterns

LATAM is a target, but the sector sees attacks trend downward globally

After explosive growth two years ago, transaction volumes for gaming and gambling grew by a more modest 7% last year, with the highest growth occurring in both North America and Latin America. As the industry becomes more regulated in these regions, a growing digital customer base continues to emerge.

Trends in the industry vary between regions, reflecting different levels of maturity around the globe. While the overall gaming and gambling attack rate was down by 9% YOY, this was driven mostly by a decreased attack rate in the more mature EMEA market. In the US, the attack rate was stable, while LATAM saw a 55% growth in the attack rate as new operators in the market were heavily tested across all areas of the customer journey—via fraudulent signup attempts, account takeovers and deposits with compromised payment instruments.

Bonus abuse and affiliate marketing fraud continue to be significant challenges during customer onboarding in many regions.

	New Account Creations	Logins	Payments
Risk Trends	We saw strong growth in the attack rates for new account creations on browser channels in all regions except North America.	The attack rate for logins decreased by 33% YOY, with decreases across all regions except for LATAM, where new accounts were targeted for account takeover (LATAM login attack rate increased by 33% YOY).	LATAM saw significant growth in the payment attack rate (up more than 600% YOY), while all other regions saw declines. Since LATAM is a small percentage of the global gaming and gambling payments, this was not enough to significantly impact the global payment attack rate, which was down 25%.
ATTACK RATE			
Overall	8.5%	0.2%	0.8%
Desktop	11.5%	0.5%	0.9%
Mobile Browser	8.7%	0.1%	0.7%
Mobile App	3.2%	0.3%	0.9%

US Government: Overview of Trends and Attack Patterns

The attack rate on government programs is skyrocketing, targeting vulnerable groups

US government fraud and cybersecurity threats, driven by domestic and international criminal organisations, are only getting worse. Data shows significant increases in bot-driven reconnaissance and account takeover attacks, while AI and deepfake technologies, pulling stolen identity data from years of data breaches, are enabling fraudsters to create synthetic identities.

Vulnerable groups like the elderly, low-income individuals, and veterans in particular are being targeted through ransomware, phishing, and state-sponsored attacks to exploit financial resources such as benefits programs.

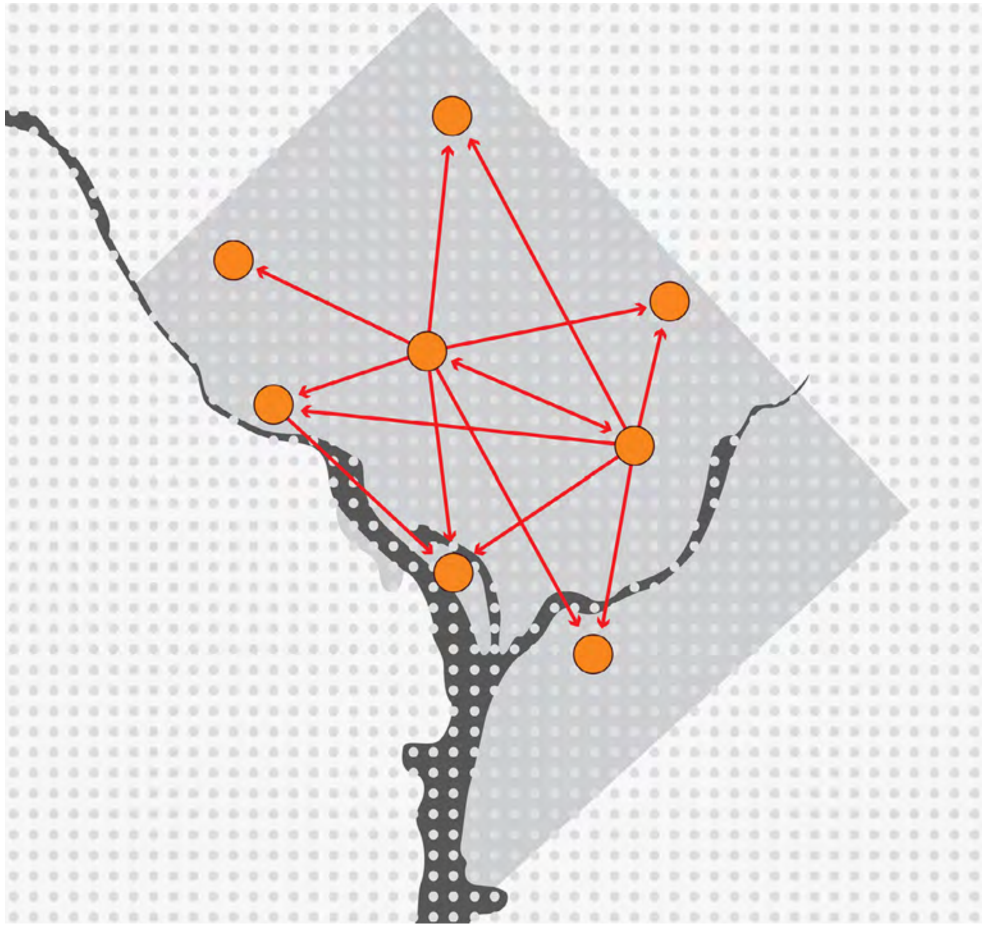
At the agency level, these attacks can target unemployment insurance (UI), the Supplemental Nutrition Assistance Program (SNAP), the Departments of Motor Vehicles (DMVs), and public education programs. Data breaches and phishing attacks can use stolen identity data to then file fraudulent claims, apply for public assistance, grants, and loans, or assume ownership of online identities—and the complexity of these agencies, especially when linked to welfare, creates additional vulnerabilities.

The overall attack rate on US government systems is 7.1%, with mobile usage at 7.3%, highlighting how lucrative new account creations are (attack rates during login events are 2.6%, aligning with the increase in account takeover attacks). Fraudsters may use text, email, and phone tactics to acquire and compromise the personal identifiable information (PII) and accounts of US citizens.

Industry standards from the National Institute of Standards and Technology (NIST) are outdated, failing to meet current best practice threat-mitigation requirements for agency identity assurance, leading to increased exploitation of government agencies. These agencies may lower security requirements to reduce user friction for disadvantaged or at-risk citizens. Without improvements in standards or changes in agency incentives, fraudsters will continue to exploit government identity vulnerabilities.

US Government	New Account Creations	Logins
	RATES OF ATTACK BY PEOPLE	
Overall	7.1%	2.6%
Desktop	6.7%	3.2%
Mobile Browser	7.3%	1.9%

Locations have been changed to anonymise the institutions involved.



● Financial Service

Each coloured circle represents a US government organisation. Each arrow illustrates digital identities, which have been associated with confirmed fraud attempts at one organisation, attempting to create new accounts at another government organisation within Digital Identity Network.

US Insurers Are Facing an Onslaught—Bots Are Already Inside

Insurers aren't just under pressure, they're under attack

More than 2,300 bots probed insurers' quote portals in the first half of last year, looking for weak spots in their digital front doors. We also saw over 12,000 confirmed fraud attempts aimed at insurers during this period—and a full half of them got through. Most didn't come from obvious threats. They looked like clean logins and real devices—easy to miss.

In one case, an insurer didn't block a single bot until the system underwent tuning to enhance detection capabilities. After three rounds, the capture rate reached 92.3%, then 100%.

That's just one battle won. It's progress, but it took months. And some insurers still have yet to take action to implement a mitigation strategy for these types of threats.

The Digital Identity Network solution tracks the same digital identities targeting many insurers. We're seeing coordinated, professional fraud across quote portals, blending in with everyday traffic patterns to evade detection.

Without shared intelligence, every insurer fights the same attackers in isolation, wasting precious time. But working together means nobody is starting from scratch. Digital Identity Network provides intelligence fuelled by data from globally contributed transactions across diverse industries.

The front line has shifted—it's time that underwriting teams treat quote portals like critical infrastructure before it's too late.

US Insurance	New Account Creations	Logins
RATES OF ATTACK BY PEOPLE		
⚠ Overall	3.5%	1.2%
Desktop	4.1%	0.7%
Mobile Browser	3.0%	2.2%

Conclusion

Make no mistake: Even though we saw no significant increase in the global rate of attack by humans, digital fraud and scam attacks remain at high levels worldwide…and the storm clouds are gathering.

A range of reports from around the globe suggest that cases are still rising, even as we see some concrete evidence that organisations with sophisticated defences and AI-optimised fraud detection policies are successfully securing their environments against these elevated threat levels.

Taking advantage of a global digital intelligence network provides forward-thinking companies with broad and deep insights into threats that can escape detection from internal data alone. More and more organisations are exploring ways to work together, within the guardrails of privacy regulations, to share resources and counter these threats.

The digital world continues to evolve rapidly, and we have to expect that fraudsters will invest more deeply in AI for 2025 and beyond. The value of this advanced technology may be limited in countries that have only recently gone through digital transformation. But in more mature digital markets, the use of AI is sure to be a disruptive force in the years to come.

Glossary, Methodology, Contact Details

Glossary

Industry Types

Financial Services includes mobile banking, online banking, online money transfer, lending, brokerage, alternative payments and credit card issuance.

Ecommerce includes retail, airlines, travel, marketplaces, ticketing and digital goods businesses.

Communications, Mobile and Media (CMM) includes telecommunications, content streaming and digital media.

Gaming and Gambling includes online gambling and egaming services.

Common Attacks

New Account Creation Fraud: Using stolen, compromised or synthetic identities, to create new accounts that access online services or obtain lines of credit.

Account Login Fraud: Attacks targeted to take over user accounts with stolen credentials available in the wild or credentials compromised by malware or man-in-the-middle attacks.

Payment Fraud: Using stolen payment credentials to conduct illegal money transfers or online payments via alternative online payment methods such as direct deposit.

Percentages

Transaction Type Percentages are based on the number of transactions (e.g. account creations, account login and payments) from mobile devices and computers processed by LexisNexis® Digital Identity Network®.

Attack Percentages are based on transactions identified as high risk and classified as attacks, by use case. Attacks are initiated by a human adversary or an automated script ("bot"). Events identified as attacks are typically blocked or rejected automatically, in near real time, dependent on individual customer use cases.

Desktop Versus Mobile

Desktop Transactions are transactions that originate from a desktop device such as a computer or laptop.

Desktop Attacks are attacks originating from a desktop device.

Mobile Transactions are transactions that originate from a handheld mobile device such as a tablet or mobile phone. These include mobile browser and mobile app transactions.

Mobile Attacks are attacks that target transactions originating from a mobile device, whether browser or app-based.

Attack Explanations

Device Spoofing: Fraudsters delete and change browser settings in order to change their device identity or fingerprint, or attempt to appear to come from a victim's device. LexisNexis® ThreatMetrix® patented cookie less device identification is able to detect returning visitors even when cookies are deleted or changes are made to browser settings. To differentiate between cybercriminals and legitimate customers who occasionally clear cookies, only high-risk/ high-velocity cookie deletions (such as a high number of repeat visits per hour/day) are included in the analysis.

Identity Spoofing: Using a stolen identity, credit card or compromised username/password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on a high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user accounts or unusual identity linkages and usage.

IP Address Spoofing: Cybercriminals use proxies to bypass traditional IP geolocation filters, and use IP spoofing techniques to evade velocity filters and blacklists. ThreatMetrix® directly detects IP spoofing via both active and passive browser and network packet fingerprinting techniques.

Man-in-the-Browser (MitB) and Bot Detection: Man-in-the-browser attacks use sophisticated trojans to steal login information and one-time-passwords from a user's browser. Bots are automated scripts that attempt to gain access to accounts with stolen credentials or create fake accounts and transactions.

Crimeware Tools: Crimeware refers to malware specifically designed to automate cybercrime. These tools help fraudsters create, customise and distribute malware to perpetrate identity theft through social engineering or technical stealth.

Low and Slow Bots: Refers to low frequency botnet attacks designed to evade rate and security control measures and thus evade detection. These attacks appear to be legitimate customer traffic, and they typically bypass triggers set around protocols and velocity rules.

Summary Methodology

- The LexisNexis® Risk Solutions Cybercrime Report is based on cybercrime attacks detected in LexisNexis® Digital Identity Network between January and December 2024, during near real-time analysis of consumer interactions across the online journey, from new account creations, logins and payments to non-core transactions such as password resets and transfers.
- Transactions were analysed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioural analytics.
- The Digital Identity Network® solution and its near real-time policy engine provide unique insight into global digital identities across applications, devices and networks. At the heart of the Digital Identity Network solution is LexID® Digital, a unique customer identifier. It provides a 360-degree view of customers by merging offline and online data in near real time to establish true digital identities.
- LexisNexis® Risk Solutions customers benefit from a global view of risks, leveraging global rules within bespoke policies that are custom-tuned specifically for their businesses.
- Attacks referenced in the report are based upon "high-risk" transactions as scored by global customers.
- North America includes the US and Canada. Mexico is included in the LATAM regional analysis.

Data Processed and Analysed

Over 120 billion transactions were processed by the Digital Identity Network solution between January and December 2024.

- The LexisNexis® Cybercrime Report analyses a subset of these transactions that excludes non-transaction-based events, (such as feedback data and test transactions), as well as transactions from organisations that are considered outliers based on extremely high or zero recorded reject rates. This subset totals 104 billion transactions.
- The Cybercrime Report uses these 104 billion transactions to calculate overall transaction volumes globally and by region. (There were 3.3 billion transactions without an IP address that cannot, therefore, be assigned to a region—these are mostly unknown sessions where an organisation does not send the input IP address.)
- This subset of 104 billion transactions is also used for analysis of automated bot attacks. This includes known sessions related to individual events, as well as unknown sessions—which can sometimes be a feature of bot traffic given that attack velocity fails to record complete profiling data.
- Human-initiated attack volumes are calculated based on a further subset of 97 billion transactions. These are categorised as "known sessions" related to individual events. This subset excludes events that failed to gather any digital identity intelligence data due to unsuccessful profiling.

LexisNexis®
RISK SOLUTIONS

For More Information
risk.lexisnexis.com/fraudandidentity

LexisNexis® Cybercrime Report
risk.lexisnexis.com/cybercrime-report

LexisNexis® ThreatMetrix®
risk.lexisnexis.com/threatmetrix

For more information, click here.

About LexisNexis® Risk Solutions
LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit risk.lexisnexis.co.uk/ and www.relx.com.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis® Risk Solutions products identified. LexisNexis® Risk Solutions does not warrant that this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis Risk Solutions. LexisNexis, the Knowledge Burst logo and LexID are registered trademarks of RELX Inc. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2025
LexisNexis Risk Solutions. NXR16887-00-0425-EN-US