Evolving Threats Beneath The Surface

How Criminal Networks Are Changing Tactics to Stay Ahead of Developing Defenses

LexisNexis® RISK SOLUTIONS

LEXISNEXIS® RISK SOLUTIONS CYBERCRIME REPORT

TABLE OF CONTENTS

LexisNexis® RISK SOLUTIONS

2026 Edition

Based on analysis of data from January to December, 2025

Global Attack Rates Are On the Rise Again

2025 saw steady digital transaction growth in LexisNexis® Digital Identity Network® globally. But fraud attacks grew faster, especially in the ecommerce and gaming and gambling sectors, pushing the global attack rate up 8% after a period of relative stability in 2024. While perhaps not yet the fraud storm that some have predicted would be driven by an AI-fueled increase in scam sophistication and automation, there are indeed signs of shifting patterns, with a much noisier identity abuse index than has been seen in recent years. Fraud is continuing to evolve around the world, regulations are being updated and fraud detection capabilities are being enhanced.

Attack growth was predominantly through browser channels, resulting in a significant shift in the balance of attacks between browser and mobile app. The volume of mobile app attacks halved in 2025, with reductions across all regions except for EMEA, while browser attacks increased dramatically. We have seen attack risk via the mobile app steadily increase the last few years, and the decline seen in 2025 may reflect that organizations are focusing on firming up their fraud detection for mobile app attacks after historically considering it a safe channel.

Bot attacks were up 59% in 2025, with growth especially targeting ecommerce and gaming and gambling. Agentic commerce was still very much in its infancy in 2025, with only small volumes of such traffic seen in the data. But traditional automated (bot) traffic was evolving, with evidence of more sophisticated simulation of human behavior. The classification of automated traffic is evolving, and organizations need to prepare for better detection and interpretation of a range of automated traffic that will surely be directed to their digital services over the months and years ahead.

As anticipated, risk associated with gaming and gambling rose considerably in 2025 (attack rate up 76% YOY), as a growing global digital customer base and the operators themselves came under attack. The industry generally saw the most transaction growth (up 20% YOY), but attacks grew much faster (up 84% YOY.) Consumer accounts are under attack in the same way as any other accounts with potential monetary value, but the digital services themselves also provide fraudsters with a range of opportunities including bonus abuse and collusion.

For the first time in several years, the EMEA attack rate rose, driven by increases in large markets such as the UK, France and Germany. Attack growth was linked to increased account takeover attempts, as fraudsters looked to exploit weaknesses in traditional 3rd party fraud prevention when defenses shifted focus to stopping authorized scams. The attack rate globally at login almost doubled (up 89%), driven by growth specifically in the ecommerce and gaming and gambling industries.

IN ADDITION TO TRENDS AND ANALYSIS FROM OUR INTELLIGENCE NETWORK, SEVERAL SPECIFIC TOPICS WILL BE EXPLORED FURTHER, INCLUDING:

- The emergence of agentic commerce
- The power of a network for reducing credit card fraud
- Cross-border fraudulent money transfer
- Collaborations and consortia in the UK

Bot attacks were up 59% this year, and the gaming and gambling attack rate rose 76%.

Global Risks

ANALYSIS OF THE JAN-DEC 2025 DATA YEAR

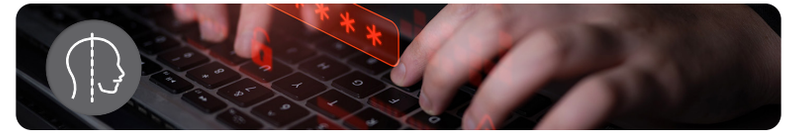
LexisNexis® Risk Solutions analyzed more than 116 billion transactions for this Cybercrime Report—a new record, and up 12% from last year. Double-digit growth continued in new account creations and payment transactions.

Global Highlights

BY TRANSACTIONS

All events analyzed in our Digital Identity Network® solution

+12% ▲	Global transaction volume YOY
+10% ▲	Financial services transactions YOY
+16% ▲	Ecommerce transactions YOY
+12% ▲	Communications, mobile and media transactions YOY
+20% ▲	Gaming and gambling transactions YOY



HUMAN-INITIATED ATTACKS

Events where the attacker is human

+8% ▲	Human-initiated attack rate YOY
-23% ▼	Financial services attack rate YOY
+64% ▲	Ecommerce attack rate YOY
-6% ▼	Communications, mobile and media attack rate YOY
+76% ▲	Gaming and gambling attack rate YOY

AUTOMATED BOT ATTACKS

Events where the attacker is code

+59% ▲	Automated bot volume YOY
+37% ▲	Financial services bot volume YOY
+123% ▲	Ecommerce bot volume YOY
+8% ▲	Communications, mobile and media bot volume YOY
+84% ▲	Gaming and gambling bot volume YOY

Attacks analyzed in our 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

Ten years of transition to mobile finally stabilizes globally

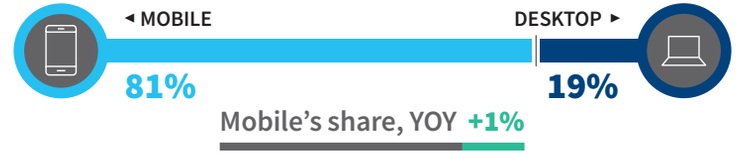
Continued strong digital transaction growth through our Digital Identity Network resulted in more than 116 billion transactions being analyzed for this report.

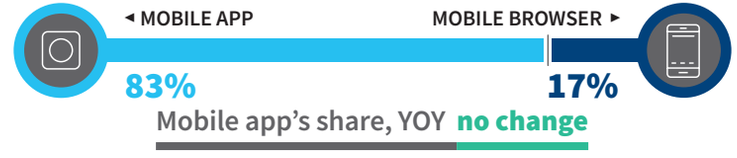
For the first time in 10 years of publishing this cybercrime report we see a fairly stable split in transactions between mobile and desktop channels (and similarly between mobile app and mobile browser). Younger generations continue to embrace all things mobile, but a not-insignificant portion of older generations remain comfortable with traditional browser-based access to digital services, and may not yet be willing to convert to mobile apps. This familiar phenomenon is well understood by traditional banks and accepted by digital banks offering an app-only service. Any organization coming to market with new digital services needs to consider this, especially if targeting the baby boomer generation as a meaningful part of their customer base.

Double-digit growth continued in 2025 for new account creations and payment transactions, while login volume growth was slightly lower than the previous year at only 8%.

For the first time, more than 10% of all transactions analyzed did not fall under the three primary use cases listed here. This reflects an ongoing focus by clients to gather as much digital intelligence as they can, at all stages of the customer journey, to help build trust and identify anomalies that could be early indicators of fraudulent activity.

TRANSACTIONS BY CHANNEL





TRANSACTIONS BY USE CASE

	▾ VOLUME	▾ CHANGE YOY
NEW ACCOUNT CREATIONS	1.4B	+15%
LOGINS	81.7B	+8%
PAYMENTS	20.0B	+13%

116.1B +12%

Our Digital Identity Network analyzed more than 116 billion transactions, up 12% YOY

Global Attack Patterns, By the Numbers

There's been a significant shift to the desktop browser attack channel

After a brief respite in 2024, the attack rate grew to 1.6% in 2025 (up 8% YOY) driven by a 19% increase in attack volume globally, with the network registering 1.8B human-initiated attacks. This may not yet be the storm that some have been anticipating now that AI tools are more readily available, both for fraudsters and for fraud prevention. However, the data suggest that the elevated state of risk that has existed since the latter stages of the pandemic has increased again this year rather than receding.

The most noticeable change in attacks in 2025 has been the 100% growth in attack rate via the desktop browser channel (rising to 4.3%) which was offset by a strong decline (down 56% YOY) in the attack rate via the mobile app channel (falling to 0.4%).

The general shift away from mobile attacks (a 30% decline, seen across all four geographic regions) has resulted in a nearly equal balance of attacks between mobile and desktop. There is no single reason for this. But as organizations have invested more in defenses for the mobile app channel, it's likely acted as an impetus for fraudsters to revert back to the traditionally easier desktop browser channels for their attacks. Browser-based services are arguably also easier to attack for emerging AI agents used for malicious purposes.

Automated bot attacks grew by 59% YOY after a small decline last year, with ecommerce and gaming and gambling bearing the brunt of the surge (attack volumes up 123% and 84% respectively). Bots that target financial services were also up sharply, doubling the growth seen last year. It remains to be seen how much of this increase in automated attacks is being orchestrated in the back end in some way by AI, even if this cannot yet be defined as agentic commerce.

HUMAN-INITIATED ATTACK VOLUME

YOY change in percentage of attacks coming from mobile devices **-30%**

ATTACK RATE		CHANGE YOY
1.6%	OVERALL	+8%
4.3%	DESKTOP	+100%
4.2%	MOBILE BROWSER	+7%
0.4%	MOBILE APP	-56%

1.8B +19% CHANGE YOY

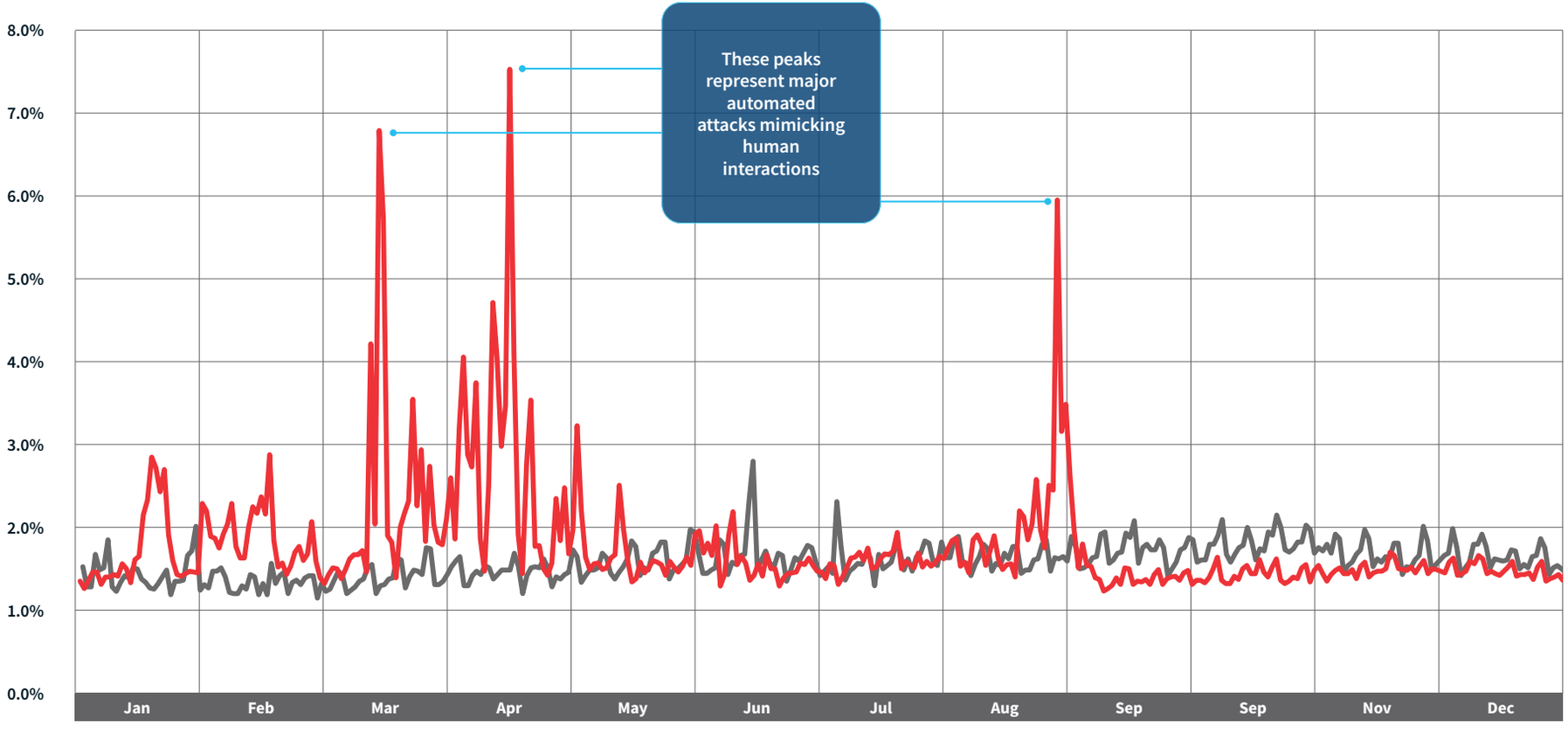
AUTOMATED BOT ATTACK VOLUME

	VOLUME	CHANGE YOY
FINANCIAL SERVICES	2.9B	+37%
ECOMMERCE	1.3B	+123%
COMMUNICATIONS, MOBILE AND MEDIA	28M	+8%
GAMING AND GAMBLING	355M	+84%

4.9B +59% CHANGE YOY

Identity Abuse Index

More noise in this year's data has contributed to a slight increase in this year's attack rate



THIS YEAR

LAST YEAR

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day, across our entire Digital Identity Network®. This includes human-initiated and sophisticated bot attacks. Unlike last year's stable index (shown in grey), there was significant fluctuation caused by major attacks in the first half of 2025 and in late August of 2025. These attacks were automated and mimicked human interactions.

Our assumption is that it's becoming easier for fraudsters to launch more sophisticated attacks, though there is no specific evidence yet to link this phenomenon to any particular AI agent. Mainly due to these peaks, the average attack rate increased by 8% YOY.

Changing Tactics

The digital world has drawn a clear line between human interactions and automated bot traffic. But 2025 introduced something different: agentic AI. Agentic commerce traffic was nearly invisible in Q1 of 2025, but had grown rapidly by Q4. Synthetic identity theft surged as well, to 11% of all reported fraud, and Card Not Present fraud continues to be responsible for major losses globally. But intelligent, organized collaboration is helping companies turn the tide.

The Fast Rise of Agentic Commerce

Agent-driven commerce has quickly moved from theory to practice, adding complexity to the threat landscape

There has been a historic focus, in the digital world, on separating human interactions from automated bot traffic. Bots simply automated a defined instruction set and were generally perceived as annoying or even malicious. Some played positive roles: Aggregators, for example, were enabled by end customers to gather account information (e.g. balances) across multiple accounts to provide a consolidated view of assets.

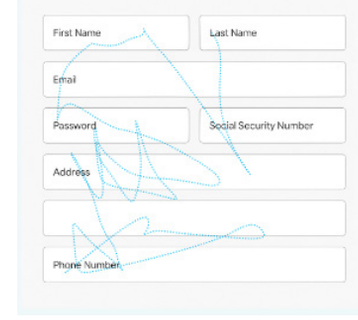
Simple bots could easily be detected by basic digital intelligence tracking a lack of human-device interaction and high IP address velocities. More sophisticated 'low and slow' bots were able to mimic basic human-device interaction and avoid simple velocity rules, but these could still be detected by more advanced data. We have tracked these in the Cybercrime Report since we started in 2015.

With the emergence of agentic AI, we are now seeing agents that can autonomously take actions and make decisions based on initial human prompts. In agentic commerce, these will ultimately emerge as a third type of interaction with digital services, with more intelligence than traditional bot traffic and working independently of the human who initially prompted their actions. The signatures of agents in digital intelligence are different from those of humans and of traditional bots, and we'll need to better understand intent as these agents become mainstream for good users as well as being adopted by fraudsters. Understanding agent intent is a rapidly evolving area that involves emerging data-sharing frameworks, across different stakeholders, that can confirm or authenticate the person behind the agent. This will continue to mature in 2026.

In our 2025 data, several things were apparent. First, we saw a significant increase in bot activity mimicking human behavior, revealed clearly by unusual peaks in the Identity Abuse Index. Second, we saw evidence of more sophisticated human behavior impersonation (through the use of Bézier curves to make mouse movements seem more natural) which we detect through enhanced behavioral analysis, as shown in the charts to the right.

Last but not least, we saw evidence of growth in agentic commerce throughout the year, starting at very low volumes in January (less than 1000 events that month) and rising 450% from Q1 to Q4 2025, as shown in the chart to the far right. Agentic traffic was almost exclusively related to online credit card payments across ecommerce sites, although a small volume was also seen on gaming and gambling sites performing account logins.

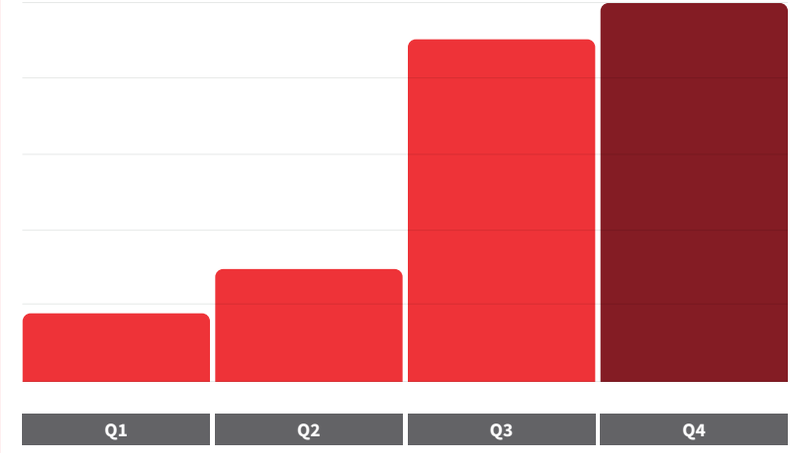
MOUSE MOVEMENT IN A HUMAN REGISTRATION



MOUSE MOVEMENT IN A SCRIPTED REGISTRATION

GROWTH OF AGENTIC COMMERCE TRANSACTIONS

(Monthly average, by quarter)



Agentic commerce grew 450% from Q1 to Q4 over the course of the calendar year.

The Power of a Network: Compromised Credit Card Data

A global view helps issuing banks identify fraudulent credit card testing faster

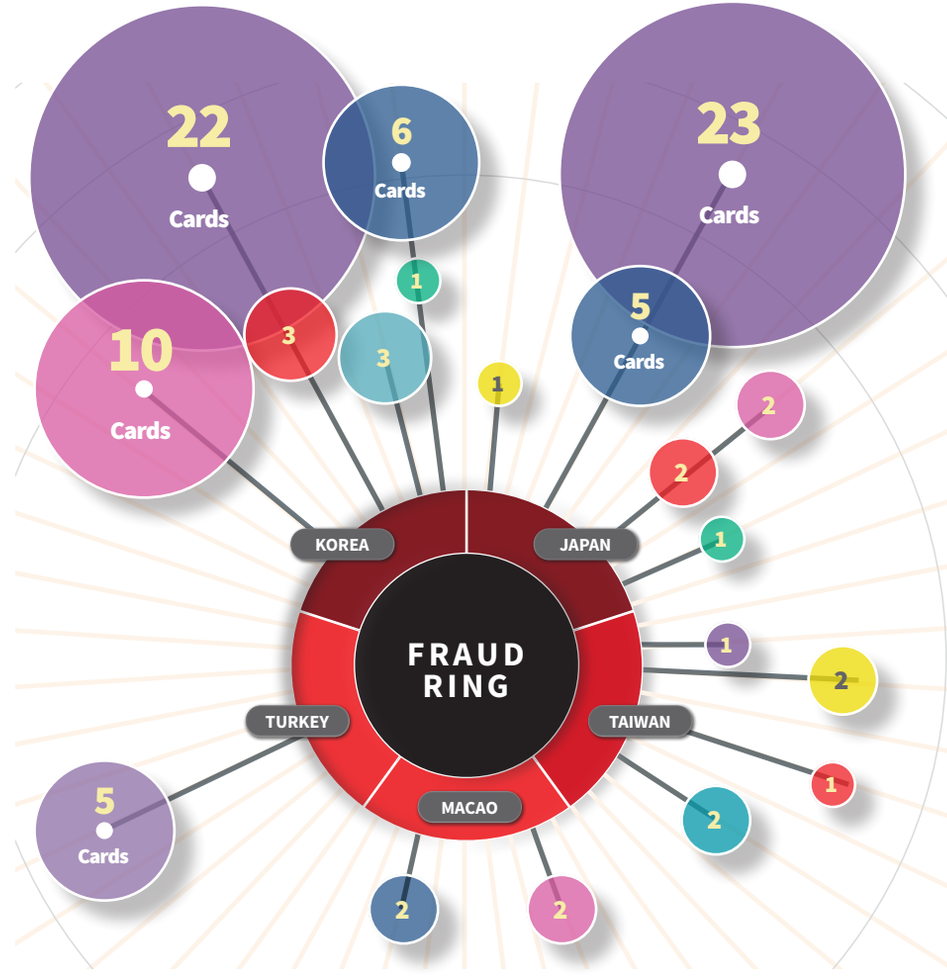
Research of illicit activity on the dark web often uncovers lists of compromised credit card data available for fraudsters to purchase. But informed collaboration can help companies defend against scaled attacks that leverage such lists, as revealed in analysis of card not present (CNP) fraud seen in the network.

The graphic to the right illustrates the activity of one fraud ring operating predominantly out of South Korea and Japan (as well as Taiwan, Turkey and Macao). This group methodically tested lists of different credit cards for a one-month period in July 2025, from a range of issuing banks including Japan, Malaysia, Hong Kong and the UAE. Of the credit cards being tested, 50% were VISA branded, 25% were Mastercard and 25% were JCB.

The ability to apply global analysis such as velocity checks across a global data set like this, regardless of issuing bank or card brand, enables issuing banks to more rapidly identify abnormal behavior and spot compromised cards being leveraged in their own customer bases.

ISSUING BANKS OF CREDIT CARDS BEING TESTED

- JAPAN
- HONG KONG
- MYANMAR
- SINGAPORE
- GREAT BRITAIN
- GEORGIA
- UAE



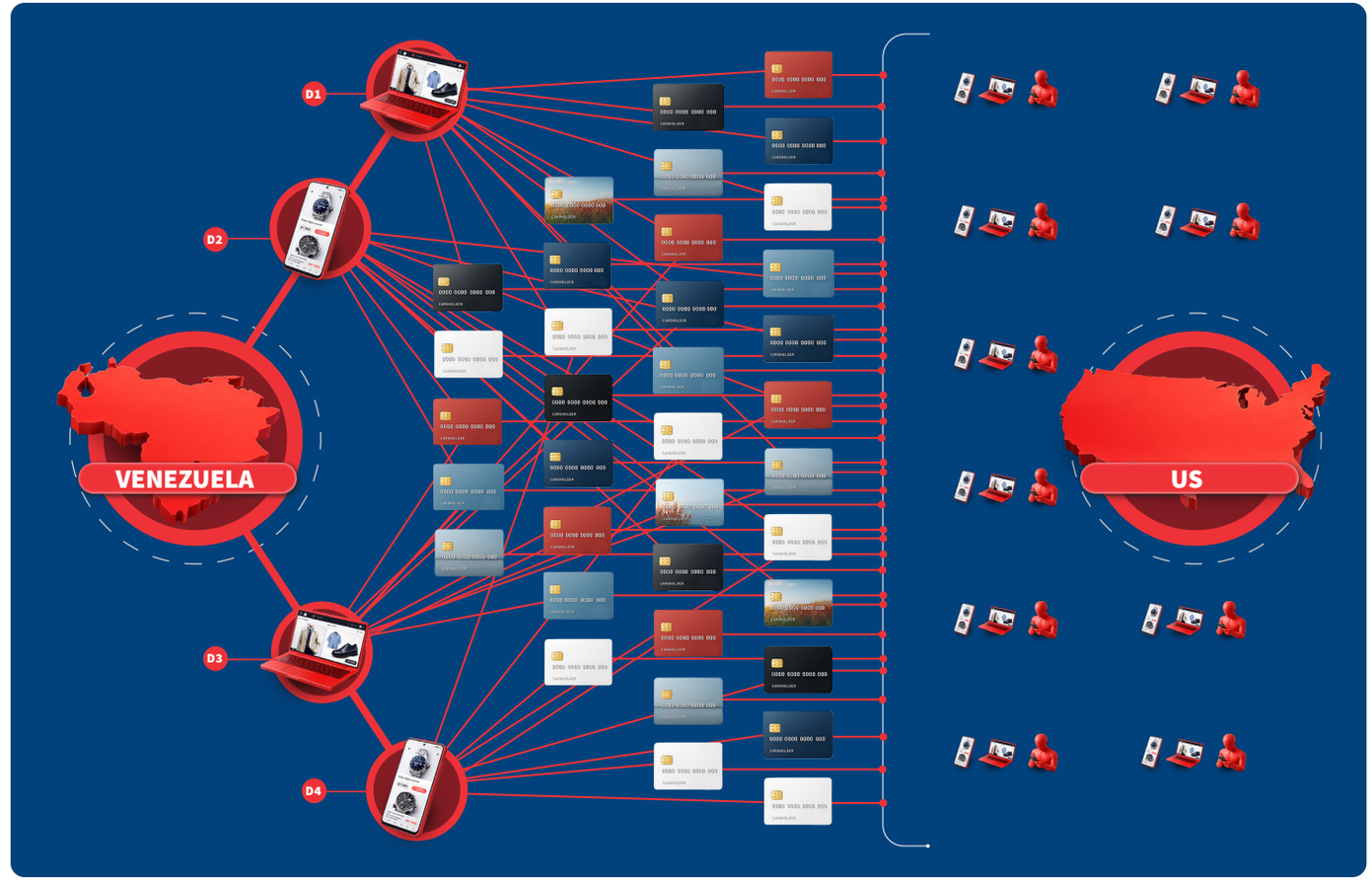
Dynamic linking of events (the diagram to the left) shows a fraud ring operating across five countries methodically testing a credit card list online. The data shows that these lists are not issuer or card network specific. Having access to a card- and issuer-agnostic global network enables faster detection of compromised card fraud.

The Power of a Network: Compromised Credit Card Data

A view across all stages of the payment journey can provide earlier fraud warnings to retailers

A valid set of compromised credit cards can be a powerful tool for fraudsters to attack retailers. In the example shown at right, a set of US merchants were targeted by a fraud ring based in Venezuela who were leveraging a list of 35 valid credit cards from different card networks and issuing banks.

Anti-fraud models can benefit from aggregated intelligence at each step of the payment journey. By analyzing data insights at merchant payment initiation, at the PSP view and finally from the issuer point of view (via the ACS service), investigators can spot signs of individual card compromise earlier. This global intelligence across the payment journey enables merchants to act earlier in the process, so they can challenge or reject payments linked to fraud rings before they succeed. The data shows that organizations are 10 times more likely to detect fraud earlier when leveraging intelligence from global digital identities in our Digital Identity Network®.



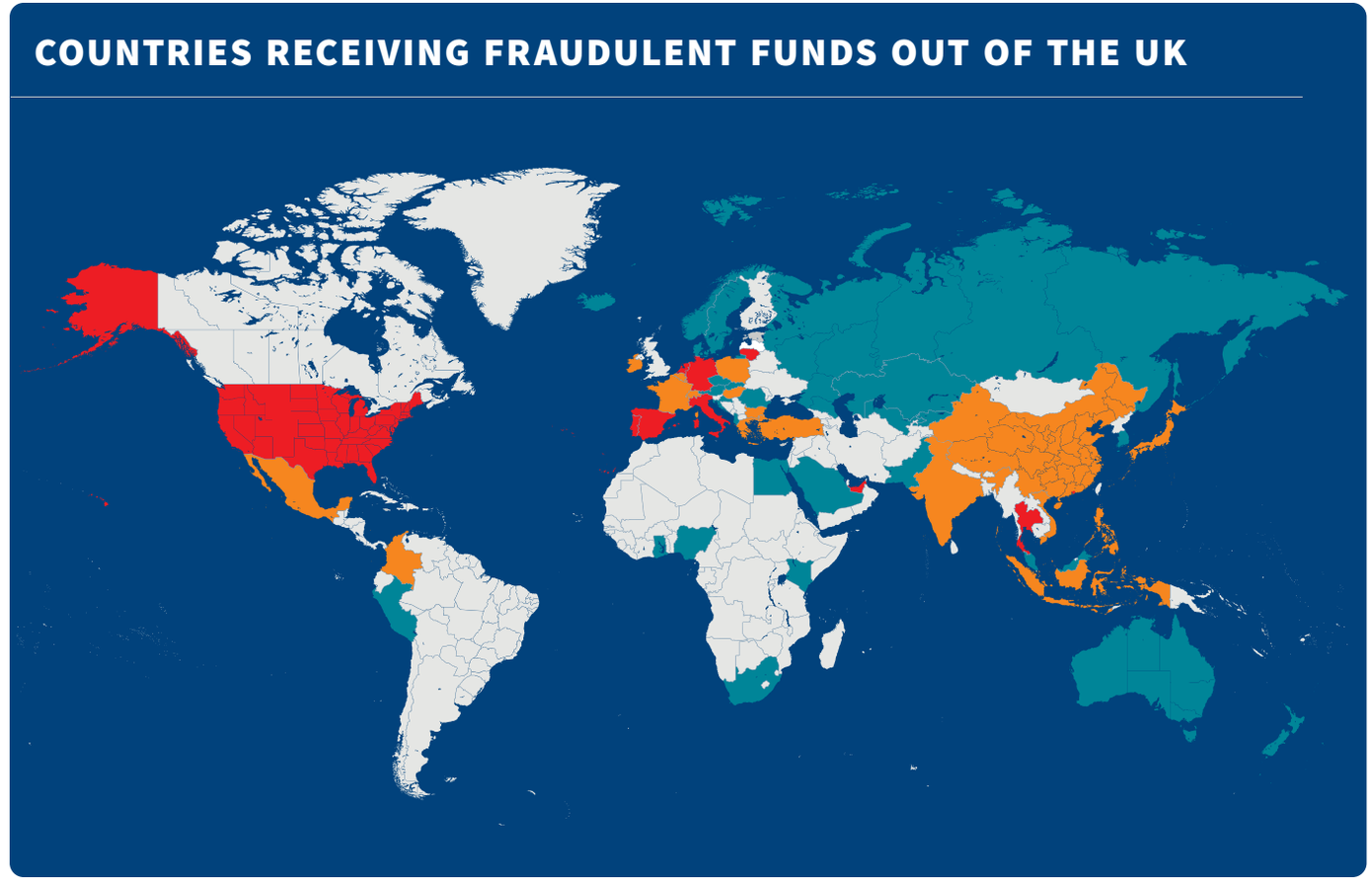
This diagram shows fraudulent attacks over a three-month period, linked by digital identity. Attacks originated predominantly from Venezuela, using 35 credit cards issued by a variety of banks to attack US retailer sites.

Cross-Border Payment Fraud: A UK Study

Fraudsters are exiting more funds abroad

We're seeing more stolen money being sent out of the UK, as fraudsters use international account-to-account money transfers in an attempt to avoid the increased fraud detection layers they're encountering on domestic transfers.

An analysis of fraudulent fund movements out of the UK, as seen in our intelligence network, is illustrated on the map to the right, highlighting countries based on the total value of fraudulent funds received from entities in the UK. Some countries are more favored than others for transferring illegally obtained funds: Our data show that Spain, the US, Portugal, the UAE and Thailand feature at the top of the list of destinations.



This chart shows the top countries to which funds obtained from online fraud in the UK are being transferred.

Cross-Border Payment Fraud: A UK Study

Fraudulent digital identities can also be analyzed to identify cross-border networks supporting fund transfers

Tracking international account-to-account money transfers provides one view of where fraudulently obtained funds are ending up. Our Digital Identity Network provides multiple ways of analyzing cross-border fraud connections.

Starting again with fraudulent activity identified at UK banks, the illustration to the right traces regions and countries where the digital identities linked to those fraud attempts have also been active. Many of these institutions are banks, but there are also several crypto exchanges and BNPL providers linked to these fraudulent digital identities, painting a broader picture of cross-border payment flows than just bank-to-bank account transfers.

Several countries seen here, such as the United States and the United Arab Emirates, also feature highly on the list from the previous page. Others, like Singapore, emerge here, and are likely destinations for fraudulent money transfers.

Providing this kind of multi-dimensional analysis of cross-border risk can improve fraud models to identify and stop more fraudulent funds from being moved out of an originating jurisdiction.

Countries Where Institutions Received UK Fraud Money

In EMEA

- United Arab Emirates, Austria, Belgium, Georgia, Germany, Ireland, Isle of Man, Italy, Latvia and Sweden

In APAC

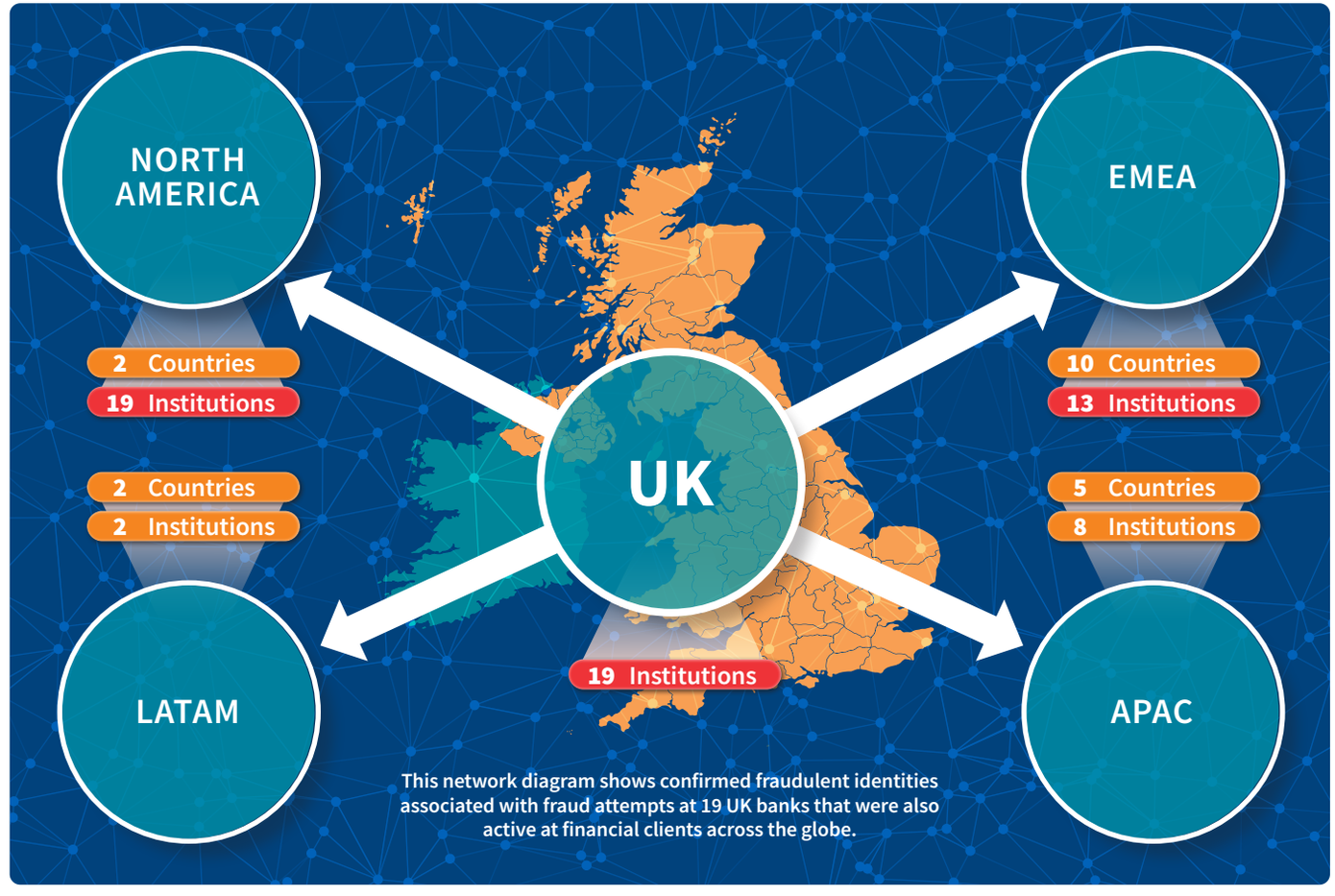
- Singapore, Hong Kong, Australia, Malaysia and the Philippines

In NORTH AMERICA

- United States and Canada

In LATAM

- Brazil and Argentina



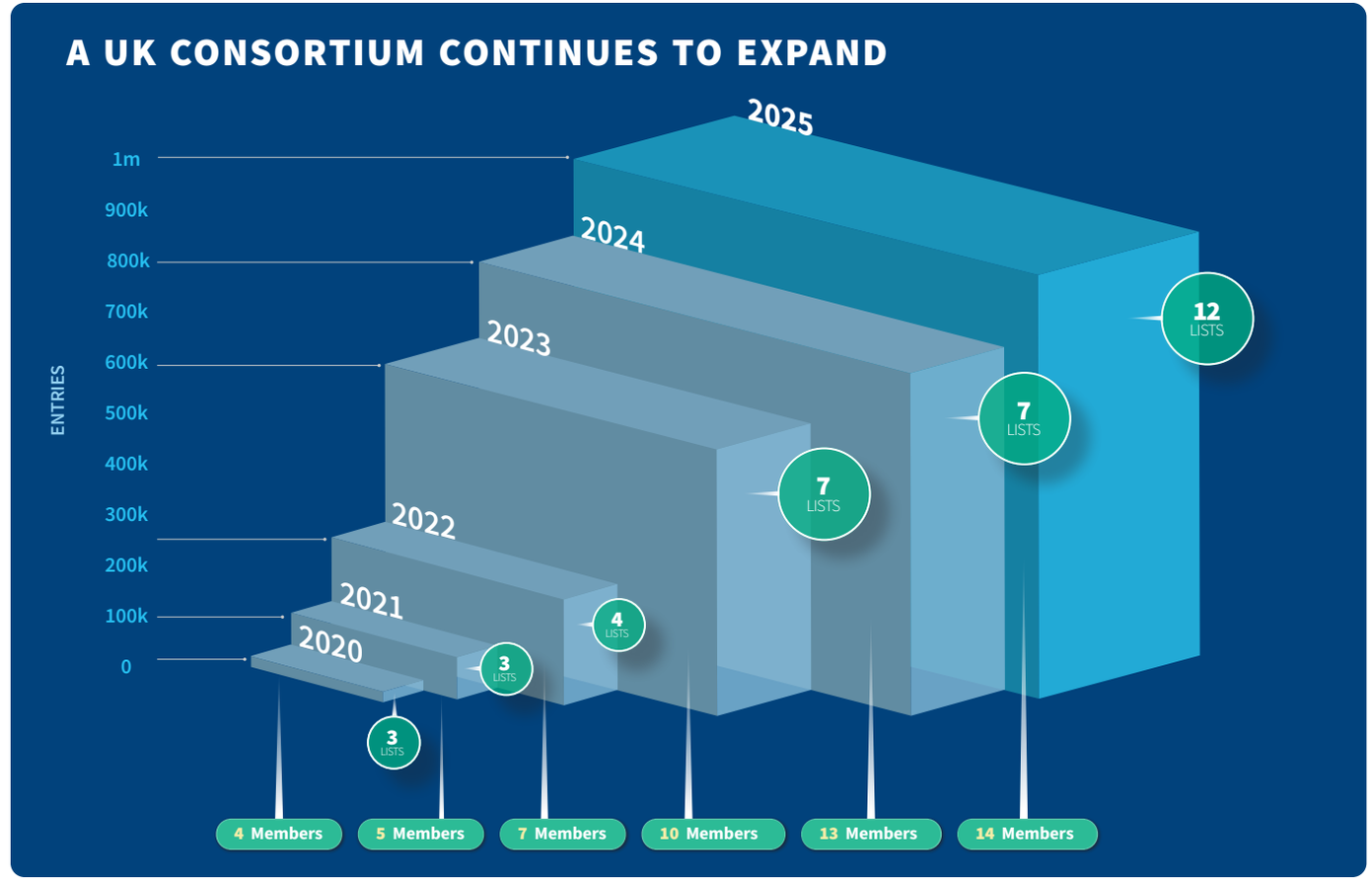
Collaboration: A Framework For Success

Consortiums take time to set up but can deliver significant value over time

Technology that enables rapid data sharing and digital intelligence can facilitate collaboration and directly influence fraud detection models. Many regulatory bodies are in the process of establishing national schemes, and private sector solutions can also provide consortium capabilities that can be deployed rapidly. We expect collaboration constructs to continue to evolve as requirements change.

The first ThreatMetrix® Consortium, established in 2019 in the UK, demonstrates the success members can achieve through active engagement coupled with clear objectives and annual review. Initially established by two Tier 1 banks, this consortium now includes 13 financial institution members, and uploads of confirmed or suspicious fraud indicators have grown from 10k to 750k+ annually.

Collaboration goes further than data sharing: It enables a community to actively engage on a regular basis, share experiences and help develop new ways of defending against emerging threats.



2020

A false positive rate of **2:1** was achieved on mule detection for 2 founding members

2021

Identifying mule networks were linked to Bounce Back Loans (BBLs).

2022

Focus on PII and beneficiary data sharing.

2023

Mule Herders initiative with UK Finance and law enforcement started. Two arrests were associated to a modern slavery ring, and **£7m** in transactions were alerted via high-risk codes.

2024 & 2025

Inter-bank notifications were established and grew to stop more mule transfers.

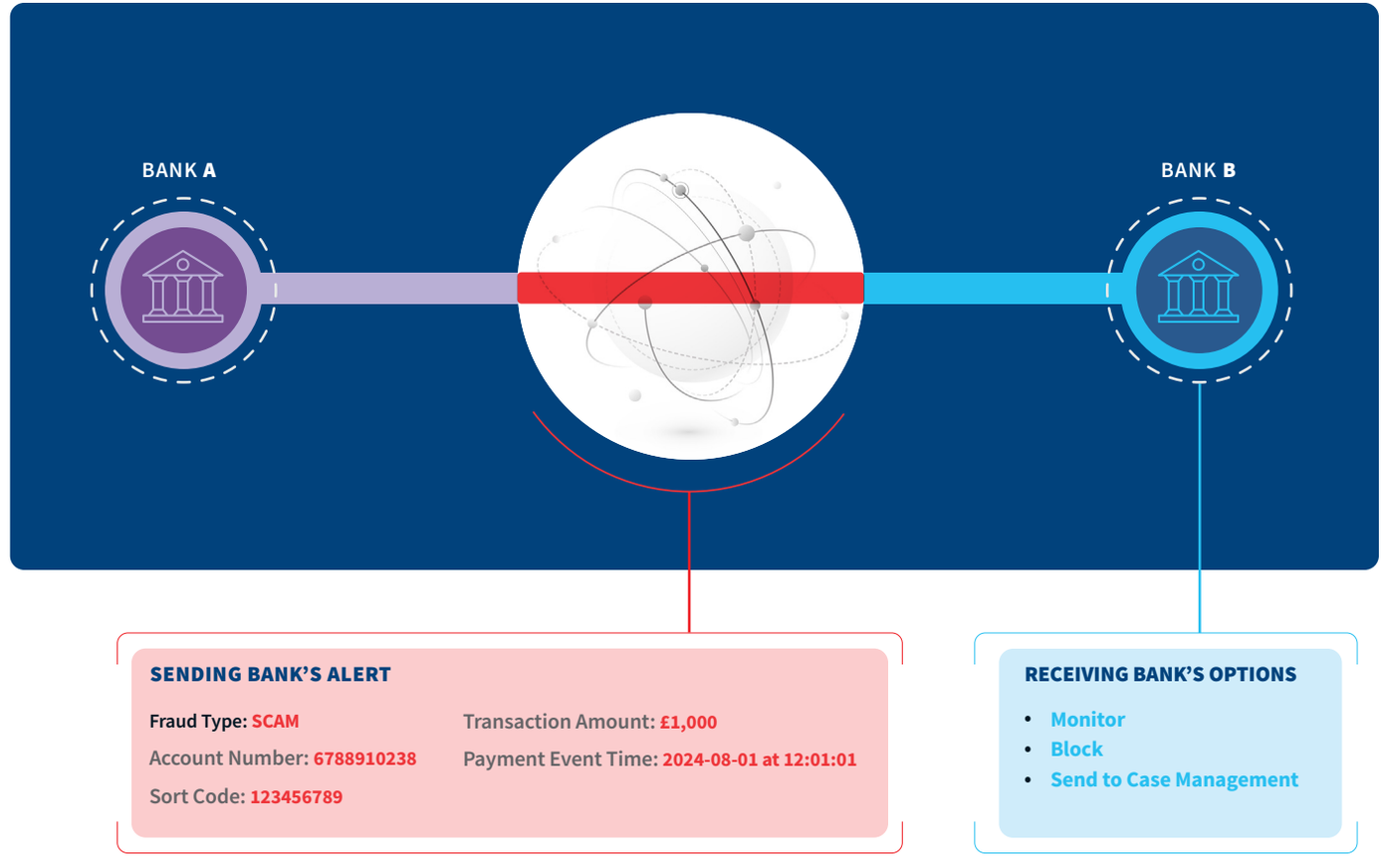
Collaboration: Inter-Bank Notifications

One bank's successful fraud intervention can serve as a warning to another bank about a mule account

As banks identify more scams in real time and block the related outgoing payments, there is a risk that the mule accounts set up to receive these payments are not identified as fast by the recipient banks, since not all scam attempts result in money arriving into the mule accounts. Collaboration through inter-bank notifications can ensure that this intelligence is still shared, even when the sending bank blocks an initial fraudulent payment attempt.

Automated notifications, triggered when bank operations teams classify a payment attempt as a scam, can enable swift alerting across a banking consortium, providing details that enable other banks to act quickly on the intelligence. These alerts are especially important in financial markets where liability for fraud losses is split between sending and receiving banks. They're also beneficial to any bank looking to improve identification of mule accounts within its own book.

Digital Identity Network data shows that when banks are using inter-bank notifications to provide rapid warning of mule accounts, between 50-70% of these notifications reveal suspected mule accounts that the receiving bank was not yet investigating.



Fraud Types From a Client Perspective

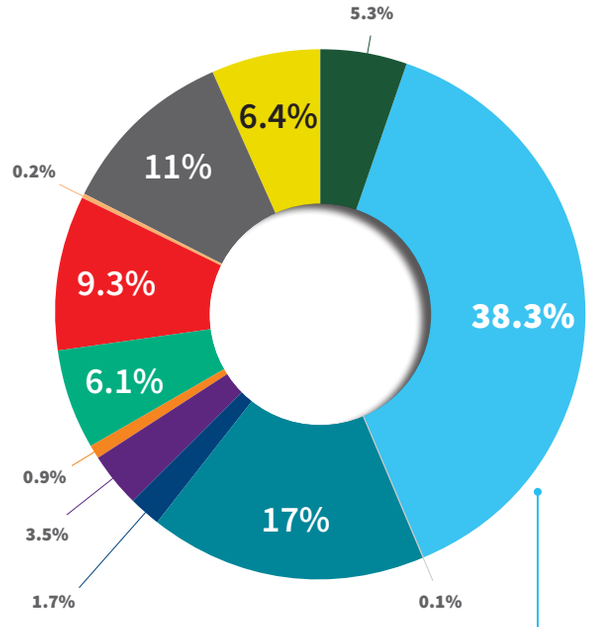
Synthetic identity fraud is rising quickly, but first party fraud further consolidates its top spot

The charts on this page show how fraud attempts in our Digital Identity Network are classified by our clients. The most prevalent categories in this year's data are first-party fraud, third-party account takeover, synthetic identity theft and scam.

We saw a significant jump in reported first party fraud in last year's report, and this trend continued in 2025, where first party fraud now represents 38% of all fraud classifications reported (up from 36% last year). Economic uncertainty around parts of the world continues to support this trend.

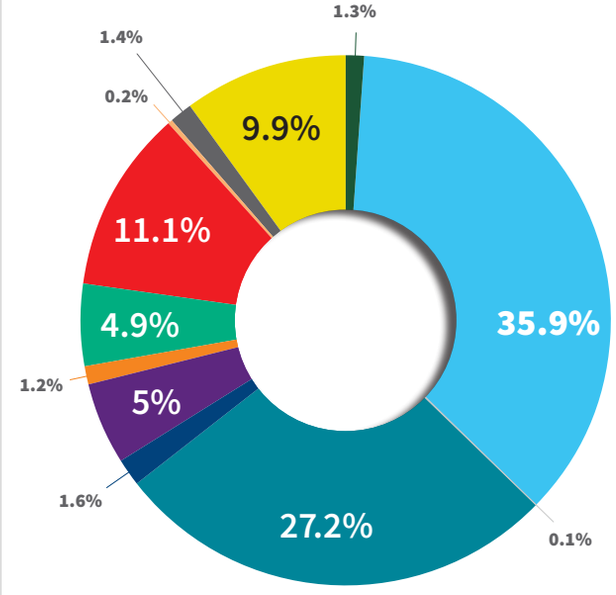
Synthetic identity theft grew significantly in 2025, and now represents 11% of all reported fraud. It has overtaken true identity theft, which declined year on year and now represents just 6% of reported fraud. Fraudsters are investing time to learn and utilize the latest technologies like generative AI to create ever more sophisticated synthetic identities that appear authentic, even including fraudulent historical backup data. Synthetic identities, once perceived as a predominantly American problem, are now very much a global issue, as seen on the next page.

THIS YEAR



Nearly two out of five frauds globally are first party fraud today—more than twice the incidence of any other type.

PREVIOUS YEAR



FRAUD GROUP

- 1st Party Chargeback Fraud
- 1st Party Fraud
- 2nd Party Fraud Collusion
- 3rd Party Account Takeover
- 3rd Party Chargeback Fraud
- Bonus Abuse
- Buyer Fraud
- Other
- Scam
- Subscription Fraud
- Synthetic Identity Theft
- True Identity Theft

Fraud Classifications by Region and Industry

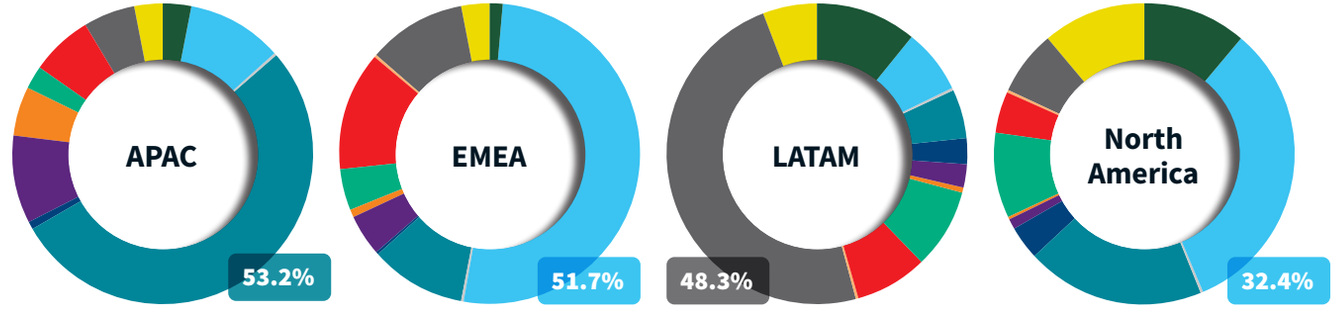
Regional fraud challenges are varied, but synthetic identities have become a global problem

Fraud classifications by clients show clear differences around the world and across industries, driven by consumer behavior, regulator influence, the maturity of fraud defenses and associated attack complexity.

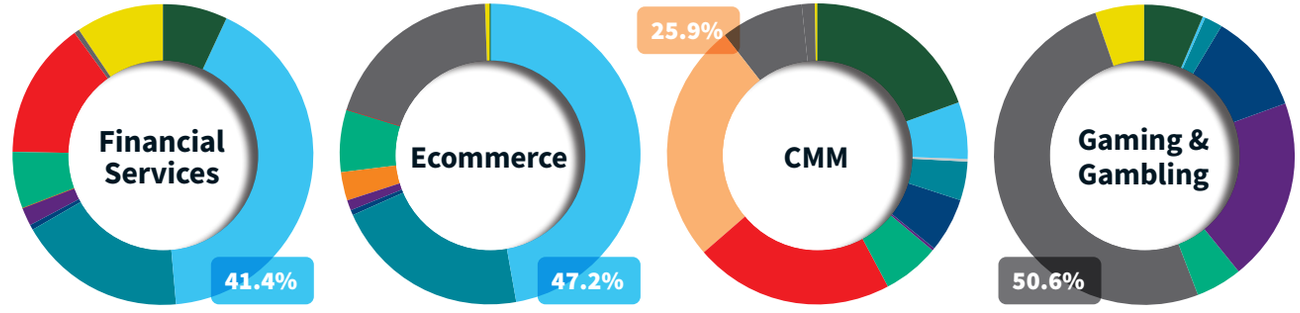
There were generally no major changes in the regional differences of fraud classifications in 2025 when compared with 2024. APAC fraud continues to be dominated by third-party account takeover, though this is driven by specific countries. EMEA and North America are seeing first party fraud attempts far outpace other fraud types. LATAM is experiencing a wide and fairly balanced range of fraud types, but reports a strong emergence of synthetic identity theft in 2025, linked to the growth of regulated gaming and gambling in the region.

The most significant change at an industry level in 2025 is that the use of synthetic identities is being widely reported in ecommerce, CMM and gaming and gambling. Of the three industries, only CMM had noted this effect the previous year (in fact, synthetic identity abuse had generally declined that year).

BY REGION



BY INDUSTRY



FRAUD GROUP

- 1st Party Chargeback Fraud
- 1st Party Fraud
- 2nd Party Fraud Collusion
- 3rd Party Account Takeover
- 3rd Party Chargeback Fraud
- Bonus Abuse
- Buyer Fraud
- Other
- Scam
- Subscription Fraud
- Synthetic Identity Theft
- True Identity Theft

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

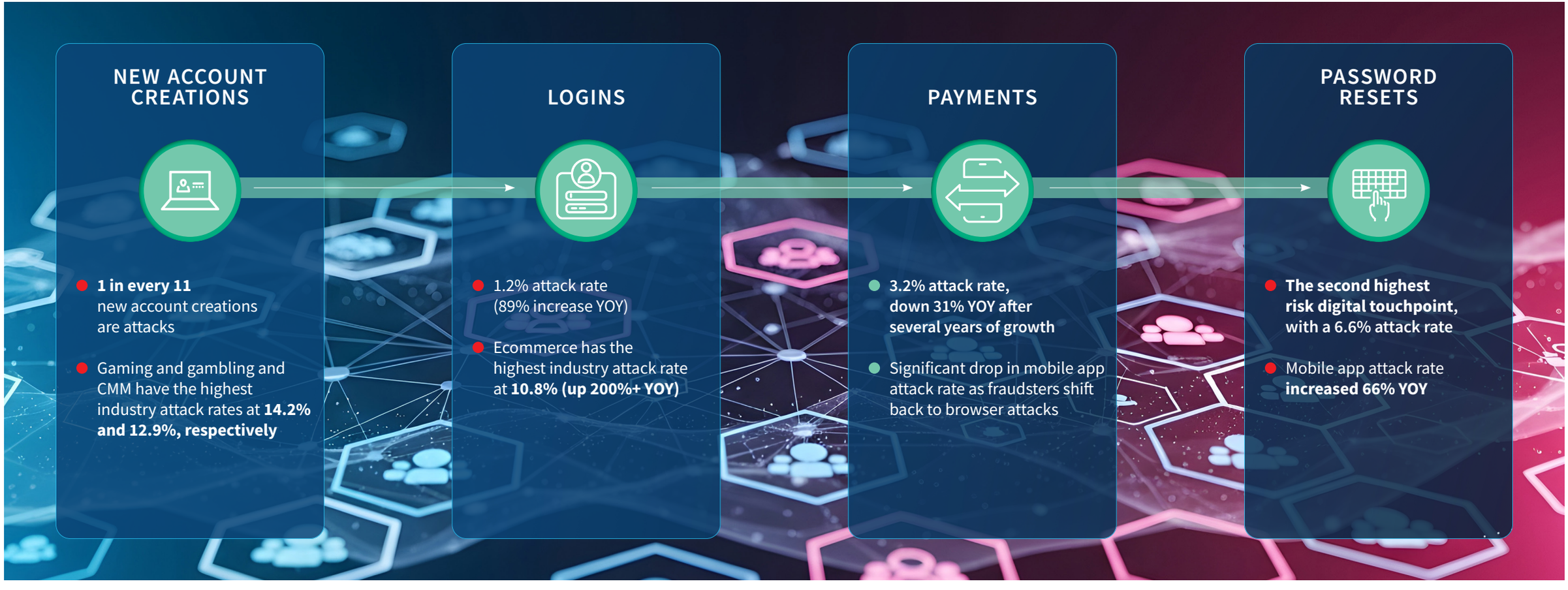
Across the Customer Journey

ANALYSIS OF THE JAN-DEC 2025 DATA YEAR

Every interaction in the customer journey represents a potential opportunity for fraud that organizations must defend against. Account creation attacks continue to be the highest-risk touchpoint, but the attack rate at login is up nearly 90% YOY, led by an astonishing rise in ecommerce attacks at login. Here's what the rest of the data says.

Customer Journey Highlights

New account creation and password reset are the most-attacked touchpoints, but the login attack rate nearly doubled this year

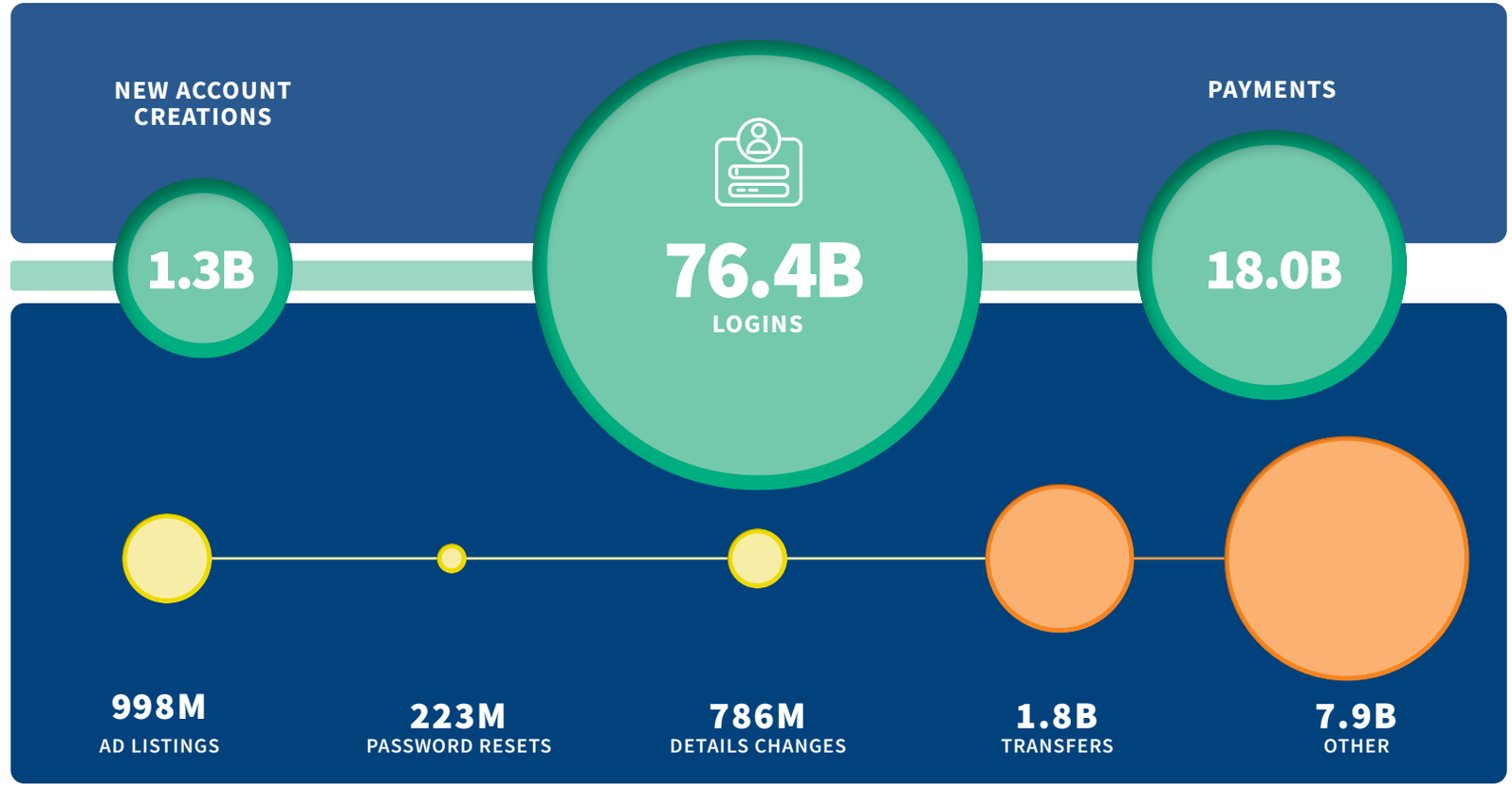


Volume of Transactions
by Use Case Across the Online Journey

Profiling risk across each customer touchpoint

Clients tend to focus on three primary stages in the digital customer journey: 1) onboarding (new account creations), 2) logins to existing accounts and 3) payments, when applicable to the digital service being offered. However, assessing additional touchpoints may be gaining traction.

As digital traffic continues to grow globally and new technologies like AI are increasingly used by fraudsters, organizations are looking to gather additional intelligence, wherever they can, to help them assess risk. For the first time this year, more than 10% of all digital events risk assessed for clients were events outside the three primary use cases named above. These events include new device registrations, password resets, changes of personal details, chatbot interactions, auction bids and online reviews, to name a few.



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

Attack Risks Across Core Touchpoints

Fraudsters renewed their focus on account takeover in 2025, while the payments attack rate declined

ATTACK RATE

RISK TRENDS

NEW ACCOUNT CREATIONS

9.0%	OVERALL
13.5%	DESKTOP
9.2%	MOBILE BROWSER
3.9%	MOBILE APP

Remaining stable at 9%, the account creation attack rate continues to be the highest-risk core touchpoint. In 2025, this also represents the highest-risk touchpoint of all types in the customer lifecycle.

The desktop attack rate increased to 13.5% (up 7% YOY), while the mobile app channel attack rate declined (down 6% YOY), a trend seen across all core touchpoints.

LOGINS

1.2%	OVERALL
4.1%	DESKTOP
2.2%	MOBILE BROWSER
0.3%	MOBILE APP

Account takeover attempts soared in 2025 after a brief decline in the attack rate in 2024. The overall attack rate, at 1.2%, is up 89% YOY, driven by more than 200% growth in the desktop channel. Gaming and gambling and ecommerce specifically saw significant growth in their account takeover attack rates.

The attack rate declined slightly in the mobile app channel, continuing the trend seen last year.

PAYMENTS

3.2%	OVERALL
4.1%	DESKTOP
5.6%	MOBILE BROWSER
0.9%	MOBILE APP

After several years of sustained growth in the payment attack rate, 2025 reversed some of these gains, leaving the overall attack rate at 3.2% (down 31% YOY).

Only the mobile browser channel saw a slightly increased attack rate, while the desktop attack rate dropped 10% and the mobile app attack rate dropped 78% to 0.9%.

The drop in the mobile app attack rate was seen primarily in the financial industry as well as in ecommerce, and was noted across all regions except for EMEA.

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

Attack rates trend downwards across other customer touchpoints

	PASSWORD RESETS	DETAILS CHANGES	AD LISTINGS	TRANSFERS	OTHER
ATTACK RATE	6.6% OVERALL	1.0% OVERALL	0.1% OVERALL	0.3% OVERALL	1.9% OVERALL
	15.1% DESKTOP	1.3% DESKTOP	0.2% DESKTOP	0.6% DESKTOP	5.0% DESKTOP
	2.2% MOBILE BROWSER	3.1% MOBILE BROWSER	0.3% MOBILE BROWSER	0.9% MOBILE BROWSER	2.6% MOBILE BROWSER
	1.1% MOBILE APP	0.5% MOBILE APP	0.1% MOBILE APP	0.3% MOBILE APP	0.6% MOBILE APP
RISK TRENDS	The password reset attack rate was down 41% YOY in 2025 to 6.6%, continuing a downward trend which started in 2024. This remains the second highest-risk digital touchpoint, linked directly to account takeover attempts. The decline was driven by a drop in the desktop attack rate (down 44% YOY), while the mobile app attack rate (at 1.1%) increased 66% YOY.	After two years of strong growth in the attack rate for details changes events, 2025 saw the attack rate plummet to 1% (down 87% YOY). This suggests that organizations have begun to identify this area of potential risk and added extra layers of defense that make this touchpoint less appealing for fraudsters. The attack rate declined significantly across all desktop and mobile channels.	Attack rates for ad listings declined again in 2025 (down 41% YOY), continuing the downward trend seen last year. Ad listings allow fraudsters to control the sale or promotion of goods and services, provide a way of monetizing stolen goods and create phony reviews to facilitate sales.	Attack rates associated with transfers continued to decline in 2025 (down 21% YOY), following a downward trend that's persisted for several years. Transfers move money into a different account within a customer's overall profile, an action that can precede a fraudulent payment event.	Clients continue to identify other digital touchpoints which can increase the digital intelligence and trust or risk that they can associate with their end customers. Other touchpoints encompassed in this category include new channel registration, standing order mandates, direct debits, beneficiary modifications and chatbot interactions. Attack rates associated with these other touchpoints remained stable in 2025.

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.

Regional Trends

ANALYSIS OF THE JAN-DEC 2025 DATA YEAR

Fraud patterns vary dramatically across the globe, shaped by regional business practices, regulatory frameworks and criminal tactics. From a rise in APAC account takeover attacks to significant ecommerce attacks in NAM, here's what we see in the data from around the world.

Regional Highlights

EMEA and APAC become growing targets, with increases in attacks outpacing legitimate transactions

APAC

+20% ▲	transaction volume YOY
+36% ▲	human-initiated attacks YOY
+39% ▲	bot volume YOY

EMEA

+8% ▲	transaction volume YOY
+36% ▲	human-initiated attacks YOY
+38% ▲	bot volume YOY

LATAM

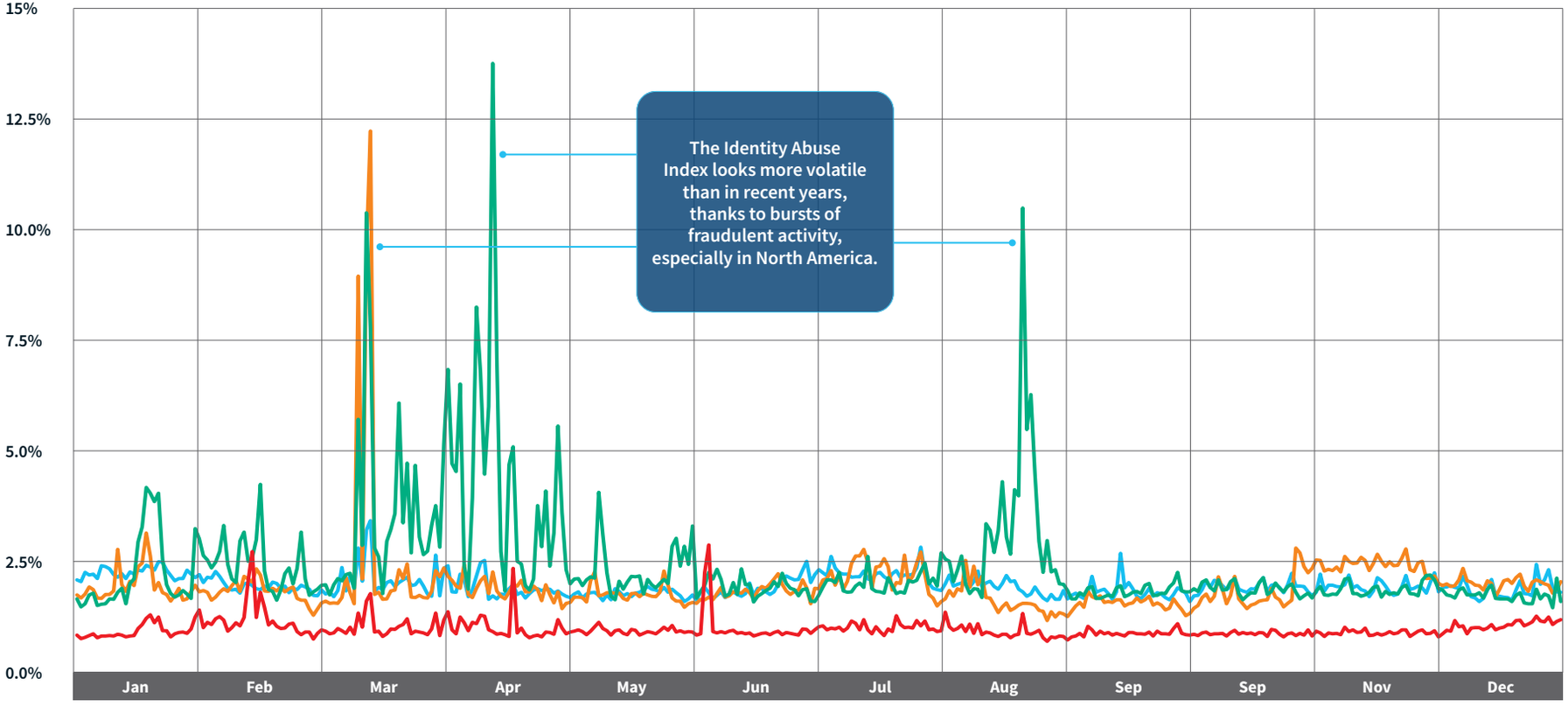
-17% ▼	transaction volume YOY
-9% ▼	human-initiated attacks YOY
+57% ▲	bot volume YOY

NORTH AMERICA

+22% ▲	transaction volume YOY
+20% ▲	human-initiated attacks YOY
+73% ▲	bot volume YOY

Identity Abuse Index by Region

Significant account takeover attacks across NAM and APAC make for an unusually noisy index



APAC's attack rate rises from 1.5% to 1.7%
The attack rate continued to grow in 2025 (up 12% YOY), with increased account takeover attempts visible during peaks in March and an elevated attack level in November.

EMEA's attack rate rises from 0.6% to 0.7%
This region saw an unusual increase in attack rate (up 27% in 2025) due to several peaks in the first half of the year and an upward trend in December. Still, EMEA remains the least-attacked region.

LATAM's attack rate rises from 1.6% to 1.7%
LATAM saw its attack rate increase by 10% in 2025 after a couple of years of decline.

North America's attack rate holds steady at 2.2%
This region saw significant ecommerce attacks several times during the year, but a low base level resulted in an unchanged attack rate year on year.

APAC
EMEA
LATAM
NORTH AMERICA

APAC Transaction and Attack Patterns

The region experiences another year of strong attack volume growth

TRANSACTIONS

VOLUME	CHANGE YOY
11.8B TRANSACTIONS ANALYZED	+20%

TRANSACTIONS BY CHANNEL

ATTACK SPOTLIGHTS

- Login attacks via desktop browser in March, coming from the Philippines and Hong Kong, targeted ecommerce accounts
- Password reset attacks on a global marketplace in October and November originated in Vietnam

ATTACKS

VOLUME	CHANGE YOY
194M HUMAN-INITIATED ATTACK VOLUME	+36%
590M AUTOMATED BOT ATTACK VOLUME	+39%

ATTACKS BY CHANNEL

YOY change in percentage of attacks coming from mobile devices **-9%**

APAC Position Against Global Figures

An evolving battle continues as fraud attacks here grow, especially on desktop

In the Asia Pacific region, the overall attack rate increased to 1.7% (up 12% YOY), taking it above the global average of 1.6%. A large increase in the attack rate via desktop browser channel (up 25% YOY, to 6.9%) was linked to more sophisticated automated attacks. At the same time, reported fraud losses in many parts of the region continued to rise.

Consumer awareness has steadily improved thanks to multiple and recurrent campaigns by local authorities. As a result, cybercriminals have adapted and changed their tactics. The use of money mules, often recruited via social media or through coercion, is now a growing problem. Regulators in countries such as Thailand, Malaysia, Singapore and Hong Kong have implemented additional measures to tackle the proliferation of money mules.

Many businesses in the regiobn have strengthened their fraud prevention strategies, and cybercriminals have adapted their modus operandi to work around fraud defenses. Recently, for instance, impersonation scams have targeted victims to execute fraudulent transactions themselves. Authorized payment scams are becoming much more common across the region. These scam cases have dealt a greater financial impact to victims and are harder to detect with conventional fraud detection techniques.

Even when regulators in the region are taking online fraud more seriously, the lack of cross-border coordination and collaboration can still provide cybercriminals with opportunities to exploit security blind spots, as bad actors are less likely to be deterred by physical or political borders.

ATTACK RATES IN APAC

	APAC	GLOBAL
OVERALL	1.7%	1.6%
DESKTOP	6.9%	4.3%
MOBILE BROWSER	4.1%	4.2%
MOBILE APP	0.4%	0.4%

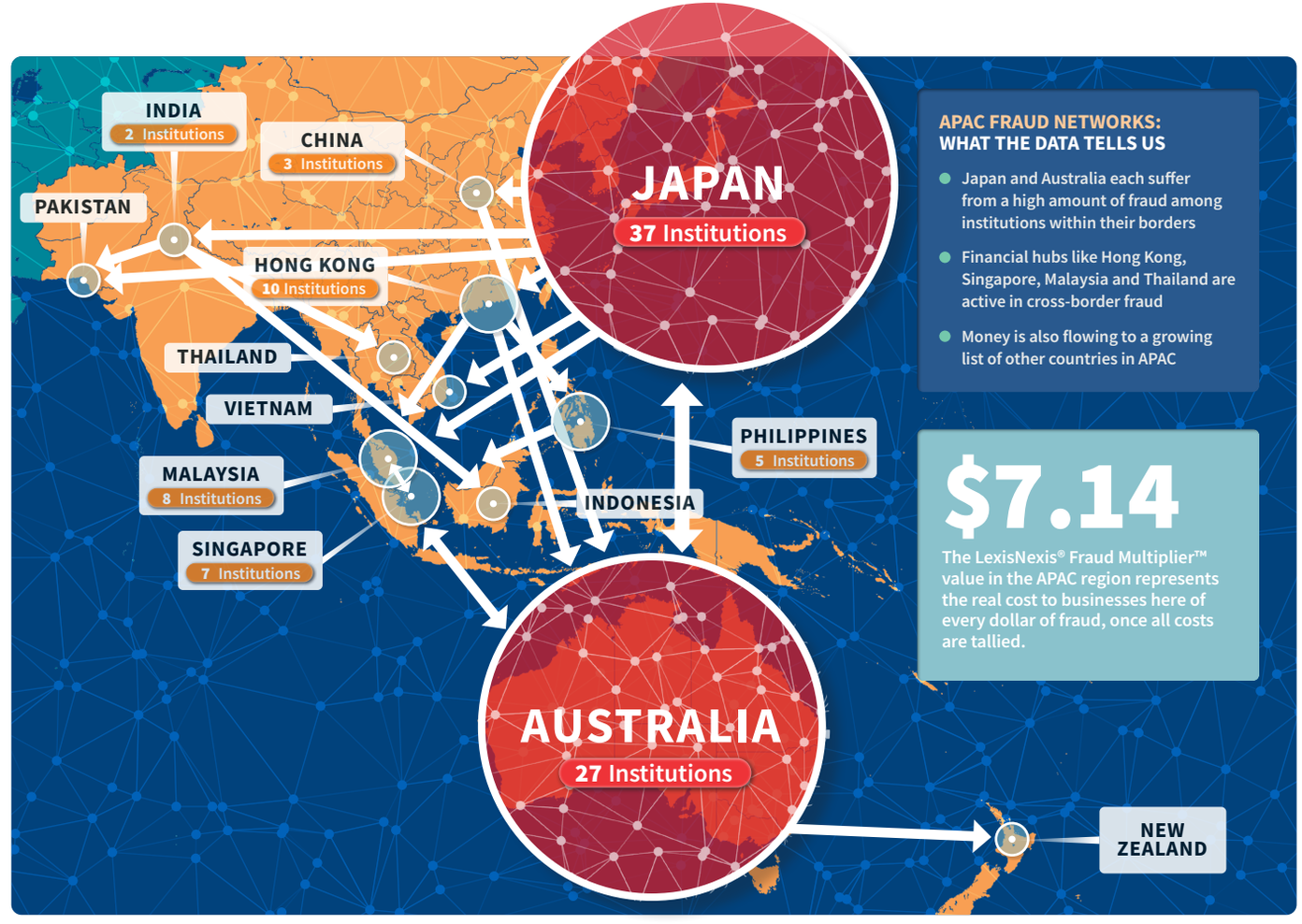
Fraud Links Across **APAC**

Regional financial hubs and insular powerhouses drive complexity here

There is considerable crossover of fraud between and among domestic organizations in Australia and in Japan, two countries with distinct locations and cultures that sometimes operate in a separate way from the rest of the Asia Pacific region. We also see clear fraudulent digital identity links that cross national borders, connecting Australia, Japan, Singapore and Hong Kong, highlighting the global nature of fraud that targets financial hubs. We also see fraud networks crossing into other countries in the region, likely highlighting money movements across borders, facilitated by instant payment systems that are increasingly linked across territories.

An effective prevention approach in the region requires local knowledge of fraud schemes at a country level as well as access to regional level digital intelligence, like the detailed data from our Digital Identity Network® seen here.

This illustration shows fraud, linked by digital identity, connected to organizations operating in APAC in the third quarter of last year. Arrow direction indicates where the activity began and then continued.



EMEA Transaction and Attack Patterns

Ecommerce accounts are increasingly under attack in the region

TRANSACTIONS

▼ VOLUME	▼ CHANGE YOY
34.3B TRANSACTIONS ANALYZED	**+8%**

TRANSACTIONS BY CHANNEL

◄ MOBILE — DESKTOP ►

87% — 13%

◄ MOBILE APP — MOBILE BROWSER ►

83% — 17%

ATTACK SPOTLIGHTS

- Frequent login attacks throughout the year via the desktop channel are targeting large ecommerce merchants. Attacks this year came mainly from the UK, Italy and Russia
- Fraudulent account creation attempts at a global marketplace originated in Finland in February

ATTACKS

▼ VOLUME	▼ CHANGE YOY
233M HUMAN-INITIATED ATTACK VOLUME	**+36%**
856.1M AUTOMATED BOT ATTACK VOLUME	**+38%**

ATTACKS BY CHANNEL

◄ MOBILE — DESKTOP ►

53% — 47%

YOY change in percentage of attacks coming from mobile devices **-14%**

EMEA Position Against Global Figures

An increasing attack rate is driven by account takeover attempts

EMEA is a large and diverse region, and the types of frauds seen here can vary by location. But there are often connections across the region, and attack patterns spotted in one place are likely to be replicated elsewhere in EMEA sooner or later.

- **In mature markets, scams are growing more targeted and sophisticated: including, for example, an employment focus in the UK linked to real estate in the UAE. Cybercrime seems to be evolving away from standard impersonation attempts, which may now be too recognizable by the general public to be effective.**
- **Digitally emerging markets are still seeing high levels of impersonation of authorities and growing attacks against new digital platforms. These attacks may sometimes focus on product launches, with fraudsters hoping to make their move before full security controls are in place.**

The declining attack rate trend seen last year in EMEA was reversed in 2025, with an increase of 27% bringing the attack rate (0.7%) back to where it was in 2023.

Significant account takeover attacks (some visible in the Identity Abuse Index) contributed to the growth in the EMEA attack rate, with the login attack rate increasing 59% YOY.

User authentication is becoming more vital to consumer protection in advanced digital markets, as emphasis on responsibility is starting to shift beyond banks to also include other parties in transactional chains, such as social media and telecoms.

Regulators are increasingly taking notice of how accounts and data are protected, not just focusing on final payments. Attack rates at login increased for ecommerce and gaming and gambling organizations specifically in 2025.

ATTACK RATES IN EMEA

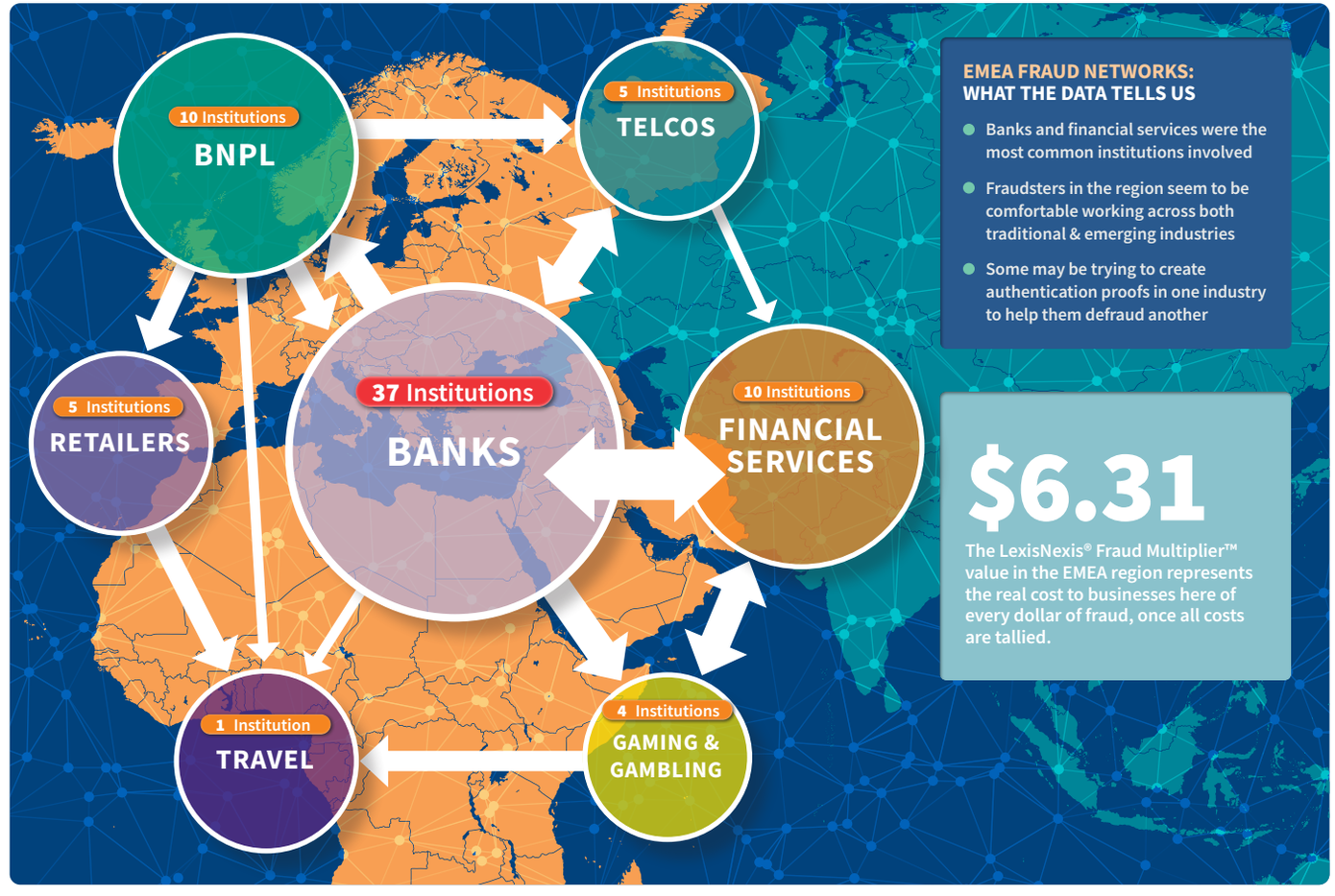
	▼ EMEA	▼ GLOBAL
OVERALL	0.7%	1.6%
DESKTOP	2.5%	4.3%
MOBILE BROWSER	2.0%	4.2%
MOBILE APP	0.1%	0.4%

Fraud Links Across **EMEA**

In the region with the lowest attack rate, fraud is growing more complex

All of the fraudulent digital identities in this view attempted to register or create new accounts at one organization, before moving on to the next. This view showcases the interconnected nature of fraud rings across traditional sectors such as finance, telecom and ecommerce. It also suggests a pattern of more complex fraud schemes, where accounts created at one organization may then be used as evidence or for authentication purposes at the next organization. For example, a fraudster might register for a new mobile phone contract ahead of applying for a loan, or might attempt to link that new phone number to an existing customer account at a bank.

This illustration shows fraud, linked by digital identity, connected to organizations operating in EMEA in the third quarter of last year. Arrow direction indicates where the activity began and then continued; arrow thickness indicates the volume of fraudulent activity seen in both locations.



LATAM Transaction and Attack Patterns

In-region and domestic attacks and automated bots are proliferating

TRANSACTIONS

VOLUME	CHANGE YOY
12.9B	-17%
TRANSACTIONS ANALYZED	

TRANSACTIONS BY CHANNEL

MOBILE 90% | DESKTOP 10%

MOBILE APP 89% | MOBILE BROWSER 11%

ATTACK SPOTLIGHTS

- Domestic account takeover attacks targeting the Brazil insurance industry occured in September
- Payment fraud attempts targeting a telco operator in June originated from Peru

ATTACKS

VOLUME	CHANGE YOY
216M	-9%
HUMAN-INITIATED ATTACK VOLUME	
537M	+57%
AUTOMATED BOT ATTACK VOLUME	

ATTACKS BY CHANNEL

MOBILE 79% | DESKTOP 21%

Percentage of attacks coming from mobile devices has decreased year-over-year -8%

LATAM Position Against Global Figures

Instant payment adoption encourages organized criminals, leading to a rising attack rate

The attack rate in Latin America grew 10% in 2025, up to 1.7% (above the global average). This rise was driven by a 31% growth in desktop browser attacks linked to automation seen across all regions. Total transaction volume for LATAM was down 17% YOY, primarily thanks to a one-time adjustment linked to a large client rather than a regional trend. This transaction reduction impacted both good customers and fraudster volumes alike, leaving attack rates (and comparisons) consistent year on year.

Latin America's fraud landscape is being reshaped by scale effects and evolving attack sophistication, particularly around instant payment systems. In Brazil alone, independent reporting shows 28 million fraud cases involving PIX recorded from January through September 2025, with digital financial crimes—such as QR scams, phishing and social engineering assisted by deepfakes – accounting for nearly 47 % of all fraud incidents logged in that period.

National security surveys estimate that 36% of Brazilians (around 61 million people) were targeted by digital scams or fraud attempts over the prior 12 months, and about 56 million reported victimization in the same period. Across these cases, accumulated losses from PIX-related scams and bogus payment schemes are estimated in the tens of billions of reais. This surge in volume and scale underscores how fraud actors are rapidly professionalizing operations, combining automation and high-touch social engineering to bypass traditional controls.

This dynamic is mirrored across other LATAM real-time rails and digital channels as well. Real world patterns show that phishing, deepfake-enhanced consent fraud and mule account networks are increasingly part of organized campaigns here that exploit both behavioral gaps and the velocity of instant payments.

As institutions and regulators work to refine countermeasures like shared risk data, advanced identity signals and layered authentication, the region is pivoting toward real-time detection and cross-institution collaboration, hoping to reduce both the number of attacks and the "average ticket" losses per event, which continue to strain consumer trust and drive policy responses. Our Digital Identity Network reveals that 98% of LATAM attacks originate within region – the highest internal attack rate across all four geographic regions.

ATTACK RATES IN LATAM

	▼ LATAM	▼ GLOBAL
OVERALL	1.7%	1.6%
DESKTOP	3.5%	4.3%
MOBILE BROWSER	5.6%	4.2%
MOBILE APP	1.0%	0.4%

Fraud Links Across **LATAM**

Travel-related fraud reveals connections across otherwise purely domestic fraud networks

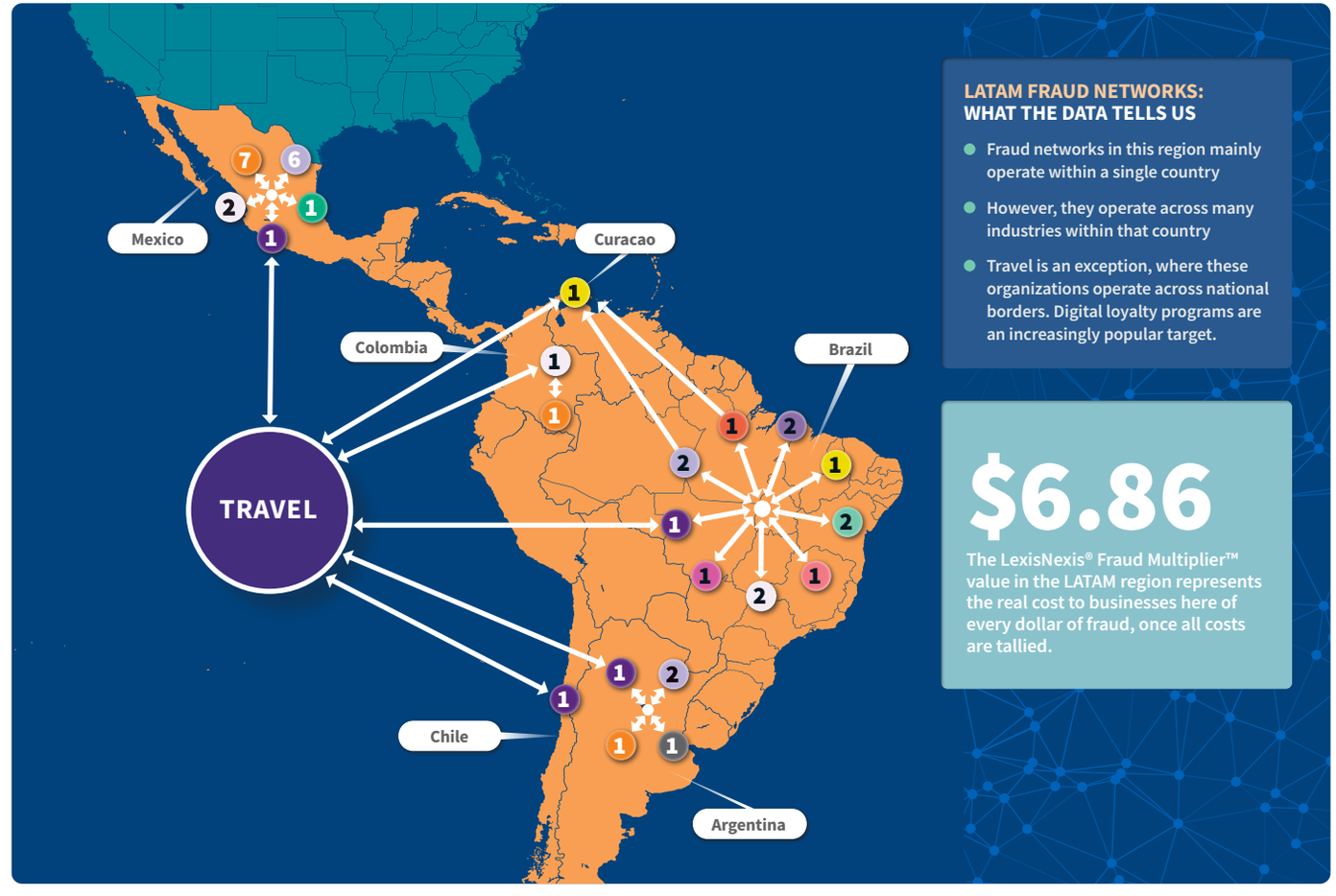
In this region, fraud networks typically operate domestically. Fraudulent digital identities in Mexico and in Brazil, for example, are generally moving from one domestic organization to another within their own country. These domestic networks link across multiple industries, from banking to retail and gaming and gambling.

The primary exception to this rule, in LATAM, is when fraudsters make use of travel sites, either for personal use or as targets for fraud attacks. Because these sites offer services across countries, they enable cross-country fraud networks to interconnect among these organizations. Travel sites still suffer from traditional fraud, like the use of stolen credit cards to purchase flights. Increasingly, though, their loyalty programs are the most lucrative targets for fraudsters looking to exploit what has effectively become a new form of digital currency.

This illustration shows fraud, linked by digital identity, connected to organizations operating in LATAM in the third quarter of last year.

INDUSTRY SECTORS

- Financial Services
- Retailers
- Buy Now Pay Later
- Gaming/Gambling
- Telcos
- Digital Banks
- Banks
- Digital Wallets
- Insurance
- Travel
- Remittance
- Payments
- Social Media



North America Transaction and Attack Patterns

Large-scale account takeover attacks against retailers occurred here in the first half of 2025

TRANSACTIONS

▼ VOLUME	▼ CHANGE YOY
53.3B TRANSACTIONS ANALYZED	**+22%**

TRANSACTIONS BY CHANNEL

◄ MOBILE — DESKTOP ►

74% — 26%

◄ MOBILE APP — MOBILE BROWSER ►

80% — 20%

ATTACK SPOTLIGHTS

- Multiple domestic account takeover attacks on a large ecommerce retailer occurred during February, March, April and again in August
- Fraudulent account creation attempts in September occurred at a telco operator via the mobile browser channel

ATTACKS

▼ VOLUME	▼ CHANGE YOY
1B HUMAN-INITIATED ATTACK VOLUME	**+20%**
2.9B AUTOMATED BOT ATTACK VOLUME	**+73%**

ATTACKS BY CHANNEL

◄ MOBILE — DESKTOP ►

45% — 55%

YOY change in percentage of attacks coming from mobile devices **-40%**

North America Position Against Global Figures

Good customers embrace mobile apps, while fraudsters are returning to the browser

North America is experiencing a significant rise in deepfakes and synthetic identities, and a rapid growth in AI-driven fraud. Concerns are rising around threat actors deploying AI agents at scale. In response, organizations are increasingly seeking sophisticated tools to accurately distinguish between attacks carried out by malicious AI agents and legitimate users leveraging AI agents to perform their tasks. Behavioral and contextual signals have become essential both for effective fraud detection and for delivering a seamless customer experience.

Unlike other regions, there continues to be a shift to mobile in North America and in particular to the mobile app channel, especially in financial services. This growth in good transactions via mobile app, together with reduced attacks in 2025 via the same channel, resulted in a significant drop in the mobile app attack rate in North America (down 77%) bringing it in line with the global average. By contrast, the traditional desktop browser channel saw significantly increased attacks in 2025 (up 165%), raising the attack rate to 4.6%, above the global average.

Scams and mule activity continue to escalate, intensifying the need for real-time risk assessment and coordinated response. Strong collaboration across institutions is becoming critical to identifying emerging patterns and mitigating threats quickly, with more organizations also seeking to leverage industry-specific and region-specific insights for strengthening collective defenses.

With good transaction volumes and attack volumes growing at approximately the same level in 2025, the overall North America attack rate remained stable at 2.2%.

ATTACK RATES IN NORTH AMERICA

	▼ NAM	▼ GLOBAL
OVERALL	2.2%	1.6%
DESKTOP	4.6%	4.3%
MOBILE BROWSER	5.2%	4.2%
MOBILE APP	0.4%	0.4%

Fraud Links Across **North America**

Strongly linked fraud networks require cross-industry collaboration to combat them

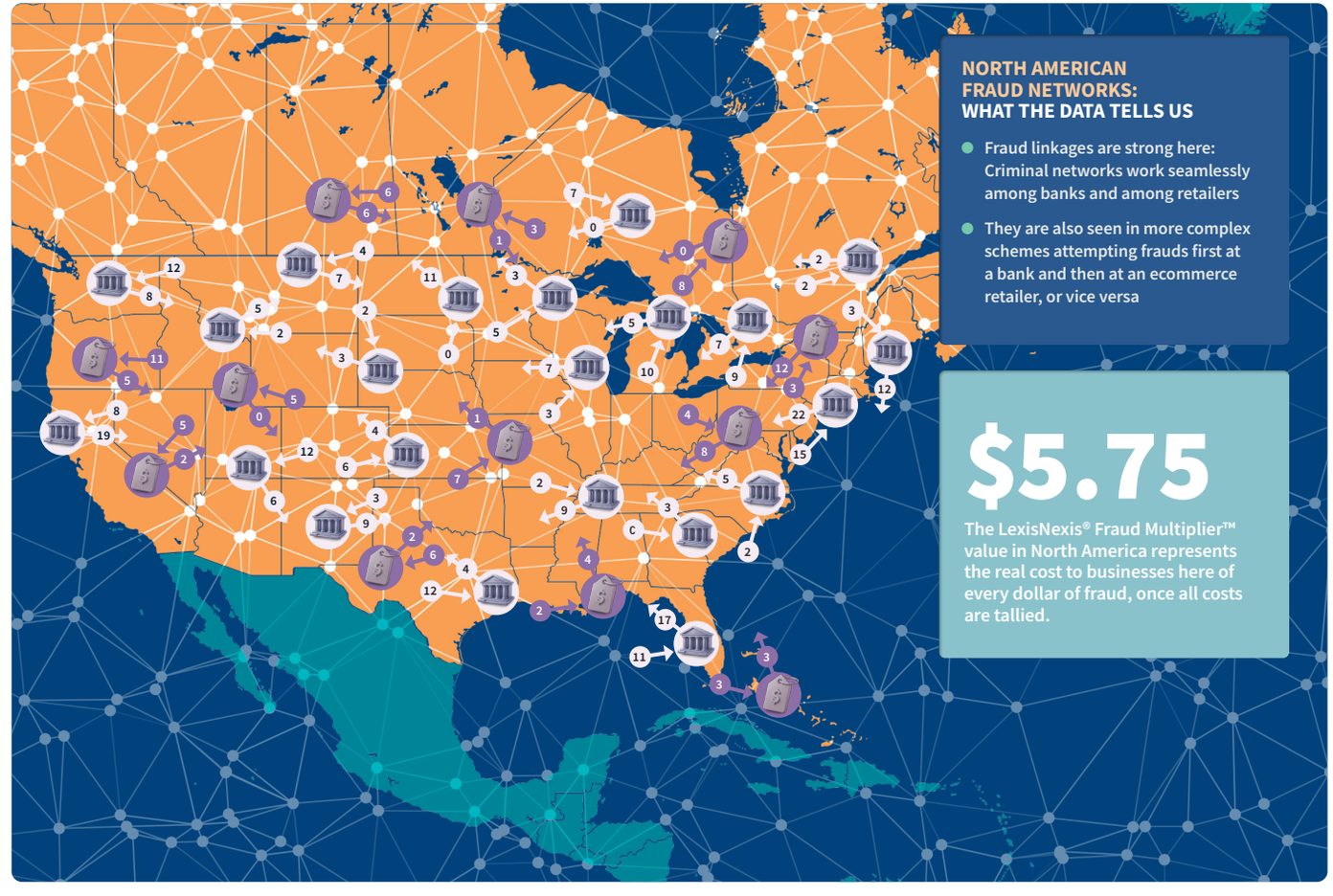
This view, of fraud connected to organizations operating in the United States and Canada as seen in the network during the third quarter of last year, showcases the interconnected nature of fraud rings in North America. Fraudsters show strong linkages not only between and among banks, but also from banks to ecommerce retailers and vice versa.

Collaboration and consortium efforts are gaining momentum at an industry level in North America. As fraud schemes here and elsewhere continue to evolve in complexity, these organizations are beginning to explore how they can best facilitate productive cross-industry collaboration.

This map shows fraud, linked by digital identity, in North American banks and retailers. Arrows pointing out signal fraud first seen at that retailer or bank; arrows pointing in signal fraud first seen elsewhere.

Retailer

Bank



Industry Trends

ANALYSIS OF THE JAN-DEC 2025 DATA YEAR

Fraud threats varied greatly by industry this year, with ecommerce suffering a 64% increase in attack rate and gaming and gambling battling a high volume of attacks during new account creation. Attack rates decreased in the financial services and in the communications, mobile and media sectors, but the overall rate increased 8% YOY.

All-Industry Overview
Trends and Attack Patterns

Significant fraud in ecommerce and gaming and gambling drive the global attack rate higher

	ALL-INDUSTRY SUMMARY	FINANCIAL SERVICES	ECOMMERCE	COMMUNICATIONS, MOBILE AND MEDIA	GAMING AND GAMBLING
ATTACK RATE	1.6% OVERALL 4.3% DESKTOP 1.0% MOBILE	1.0% OVERALL 1.8% DESKTOP 0.8% MOBILE	4.6% OVERALL 11.2% DESKTOP 2.0% MOBILE	5.2% OVERALL 4.5% DESKTOP 5.4% MOBILE	1.7% OVERALL 2.0% DESKTOP 1.7% MOBILE
RISK TRENDS	The overall human-initiated attack rate (1.6%) increased by 8% YOY in 2025, driven by strong increases in the attack rate in the ecommerce and gaming and gambling sectors.	The global financial services attack rate was down 23% YOY in 2025, due to significant decline across the mobile channel, while the desktop attack rate actually saw a slight YOY increase.	There was an exceptional rise in the ecommerce attack rate in 2025, which climbed 64% YOY to reach 4.6%. (Only the gaming and gambling attack rate grew faster.) Attack growth came via the desktop browser channel, which was up 168% YOY.	CMM still has the highest attack rate by industry, but 2025 saw the first decline in that rate since 2022. In particular, a decline in the mobile attack rate resulted in an overall CMM attack rate of 5.2%.	As anticipated with the growth in regulated digital gaming and gambling globally, the attack rate here increased significantly (up 76% YOY) to 1.7% in 2025.

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.

Financial Services
Overview of Trends and Attack Patterns

A decline in financial services' attack rate is likely linked to a focus on mobile app security

In 2025, financial services transactions in our Digital Identity Network® grew at 10% (slightly slower than the 16% seen in the prior year). Growth was driven primarily by the mobile app channel, with traffic up 11% YOY compared to 3% growth in desktop browser traffic.

The attack rate was down 23% in 2025 after being relatively stable in 2024, with both North America and APAC showing a decline. This decrease was driven by a significant decline in the mobile app attack rate, though this was offset by growth in both desktop and mobile browser channel attack rates. The effect was amplified by stronger growth in trusted transactions in the mobile app channel compared to browser-based traffic, an effect seen predominantly in North America and APAC.

The risk of potential mobile app channel fraud has been highlighted for several years in this report. The assumption is that as financial institutions have increased focus on mobile app security, fraudsters have pulled back from this channel, and turned back to the traditionally more vulnerable desktop browser channel.

ATTACK RATE

RISK TRENDS

NEW ACCOUNT CREATIONS

6.5%	OVERALL
8.1%	DESKTOP
8.0%	MOBILE BROWSER
3.9%	MOBILE APP

The decline in attack rate for new account creations in financial services continued in 2025, down 8% to 6.5%. A declining attack rate was seen across all channels.

LOGINS

0.4%	OVERALL
1.1%	DESKTOP
1.0%	MOBILE BROWSER
0.2%	MOBILE APP

The attack rate for logins decreased slightly (down 9% YOY) in 2025, with a decline in mobile channels being partly offset by growth in the desktop channel attack rate.

PAYMENTS

3.9%	OVERALL
5.4%	DESKTOP
7.2%	MOBILE BROWSER
0.5%	MOBILE APP

The payment attack rate fell by 36% YOY to 3.9%, driven by significant decline (down 90% YOY) via the mobile app channel.

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.

Ecommerce

Overview of Trends and Attack Patterns

This sector is seeing renewed focus on fraudulent takeovers of existing customer accounts

While ecommerce growth was strong in 2025 (transaction growth up 16% YOY in our Digital Identity Network), choice for the customer has also grown. Merchants are increasing focus on customer retention and loyalty, and using AI to improve and personalize the customer experience.

Attacks grew faster than legitimate customer transactions, leading to a 64% increase YOY in the attack rate for ecommerce – a much more significant rise than we've seen over the last few years. The number one target was customer accounts, with the account takeover attack rate up 216% YOY.

While this growth was seen across all regions, it was particularly severe in APAC and North America. Factors contributing to this attack rate growth could include data breaches coupled with sophisticated fraud tactics and less securely protected account access (perhaps initiated in the service of increasing seamless experiences for end customers). Bot volume specifically targeting ecommerce also rose (up 123% YOY).

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK RATE			
	8.2% OVERALL	10.8% OVERALL	2.0% OVERALL
	17.3% DESKTOP	16.9% DESKTOP	2.3% DESKTOP
	5.1% MOBILE BROWSER	6.9% MOBILE BROWSER	2.1% MOBILE BROWSER
	3.6% MOBILE APP	2.0% MOBILE APP	1.7% MOBILE APP
RISK TRENDS	The new account creation attack rate for ecommerce rose 10% YOY (up to 8.2%), primarily driven by an increase in the already elevated desktop attack rate (up 18% YOY, to 17.3%).	Account takeover remains a key focus for fraudsters in ecommerce, with the login attack rate jumping to 10.8% from 3.4% last year (a 216% increase YOY), supported by more sophisticated automation of attacks targeting the desktop channel.	The attack rate on ecommerce payments declined 24% YOY (to 2.0%), slowing across all three channels as fraud defense shifted focus to login compromise.

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.

Communications, Mobile and Media

Overview of Trends and Attack Patterns

CMM enjoys a welcome respite this year, as tighter controls start to dissuade fraudsters

The communications, mobile and media (CMM) attack rate declined 6% last year, after several years of sustained growth. The number of telco operators joining our Digital Identity Network® has grown significantly over the last five years, as operators, seeing their services actively targeted by fraudsters as part of complex scams, embrace digital intelligence as an extra level of protection. When digital defenses tighten, fraudsters often become dissuaded and look for easier prey.

At the use-case level, payments was an anomaly as it saw an increase in the overall attack rate (5.6%), and across all three channels. While fraudsters may be less successful in creating accounts for use in sophisticated attacks elsewhere, they are still looking for ways to take advantage of stolen payment instruments. For example, we see them leveraging one-off credit card payments that can be made in niche mobile or media service offerings, as opposed to regular telco operator contract services.

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK RATE	12.9% OVERALL	0.7% OVERALL	5.6% OVERALL
	22.8% DESKTOP	0.7% DESKTOP	10.3% DESKTOP
	11.3% MOBILE BROWSER	0.8% MOBILE BROWSER	6.1% MOBILE BROWSER
	3.3% MOBILE APP	0.03% MOBILE APP	4.5% MOBILE APP
RISK TRENDS	The CMM attack rate (12.9%) at onboarding was stable this year, with only the mobile app attack rate declining. The overall attack rate remains high, with only gaming and gambling experiencing similarly high attack rates at new account origination.	The login attack rate for CMM was relatively stable in 2025, slightly down from last year's number. At the channel level, the desktop attack rate jumped 92% YOY, but this was offset by declines in both mobile channels.	While the attack rate for payments in some other industries was down YOY, for CMM the attack rate rose sharply (up 84% YOY), to 5.6% across all channels.

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.

Gaming and Gambling
Overview of Trends and Attack Patterns

Around the world, fraudsters are focusing efforts on this fast-growing digital industry

The online gaming and gambling market continues to grow strongly, with transactions up 20% YOY – the highest growth by industry seen in our Digital Identity Network® in 2025. Global growth has been driven by several factors including ongoing regulatory changes opening new markets, a rise in interactive experiences enabled by the latest smart phones, AI and virtual reality and wider availability of cryptocurrency-based gambling platforms.

The attack rate for gaming and gambling went up significantly in 2025 after remaining fairly stable for a few years. All regions saw significant increases, especially North America, as fraudsters consolidate their efforts on this industry across all parts of the customer journey.

Aside from new account takeovers, this year has also seen strong growth in the use of synthetic identities during new signups. This is a significant development, driving the overall attack rate for new account creations up to 14.2%.

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK RATE	14.2% OVERALL	0.4% OVERALL	2.1% OVERALL
	26.0% DESKTOP	1.0% DESKTOP	1.7% DESKTOP
	14.7% MOBILE BROWSER	0.3% MOBILE BROWSER	2.1% MOBILE BROWSER
	4.9% MOBILE APP	0.8% MOBILE APP	2.3% MOBILE APP
RISK TRENDS	2025 saw a significant increase in attacks on gaming operators, as fraudsters tried creating new accounts with stolen and synthetic identities. The overall attack rate at new account creation increased to 14.2% (an increase of 68% YOY). Attack rate grew for all channels, especially desktop (up 126% YOY).	The account takeover attack rate increased by 163% YOY in 2025 reaching 0.4% as fraudsters attempted to compromise digital accounts created relatively recently. The mobile app channel saw the greatest increase, rising 216% YOY to reach 0.8%.	In line with the other two core use-cases, the payment attack rate for the gaming and gambling sector increased significantly this year, up 170% YOY to 2.1%. All channels saw significant increases in the attack rate.

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.

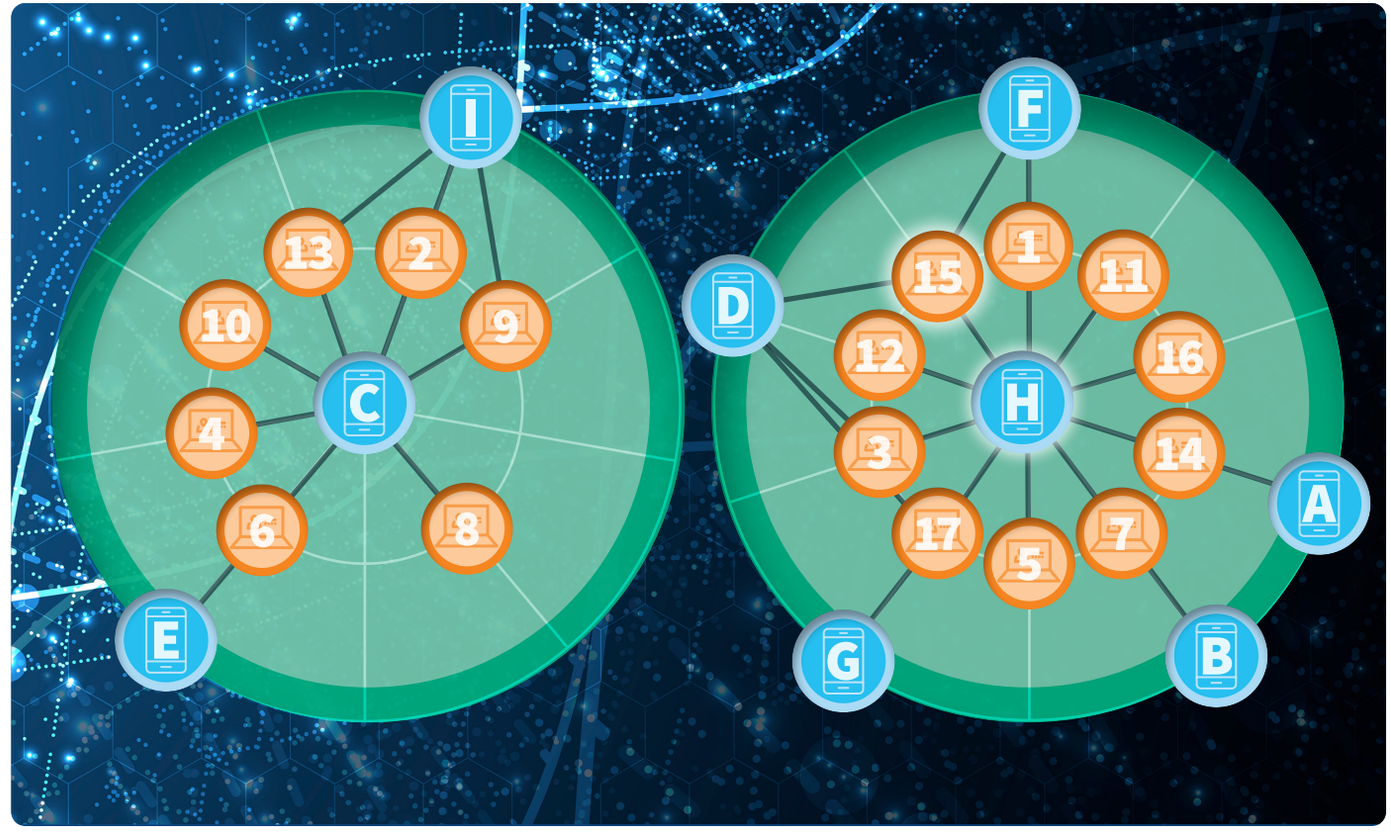
Health Insurance

Overview of Trends and Attack Patterns

Fraudsters are employing multiple devices and accounts in complex healthcare attacks

Health insurance fraud is a global issue. While digitization of insurance services has raised the potential for making fraud easier to commit, it has also become easier to detect when insurers deploy the correct layers of digital intelligence to look for the telltale patterns or signatures of fraud.

There are many different types of health insurance fraud, potentially involving a variety of actors. Common examples can include identity swapping (when an insured individual shares his/her ID with another individual who is not insured), fraudulent reimbursement (where a clinic requests payments to cover procedures that did not actually take place, potentially in collusion with the patient) and misrepresentation of procedures to obtain reimbursement for procedures not covered by a particular health plan (for example, cosmetic surgery). In addition to these, attacks can also target patients to gain access to their accounts and sensitive medical records.



Devices (A-I)

Accounts (1-17)

In this illustration, two fraud networks show confirmed fraud events (claims fraud and two-party fraud types) that are associated with specific health insurance accounts. Both of these networks showcase two relationships:

1. Multiple accounts being accessed by a single device (example: Device H), suggesting abuse of accounts by a single fraudster.

2. Individual accounts being accessed by multiple devices (example: Account 15), suggesting potential account swapping.

These frauds occurred during a single two-month period, involving 9 devices operating across 6 cities, 17 accounts and 230 individual fraud events.

Conclusion

The population of the world continues to be under attack. Fraud attempts and scams of increasing sophistication are continuously scouring defenses for weaknesses, so they can target the vulnerable, the uninformed or innocent people simply caught out in a moment of distraction. The Identity Abuse Index only rose modestly (by 8%) this year, but it showed an unusually high level of nontrivial fluctuations in the first half of the year.

Despite several well publicized raids, scam centers around the world continue to expand and flourish. The sheer number of people involved in this mature, industrialized business is a challenge to fraud prevention departments globally. The increasing availability of tools fraudsters can use to automate and improve their fraud attempts further compounds the problem. As society experiments with the likes of ChatGPT and Claude, fraudsters are undoubtedly on a parallel journey of discovery and experimentation with the new tools at their disposal. It's all moving very, very quickly.

And yet the world fights back. In every region, new security solutions are being pioneered; regulations are being tightened; scammers are being arrested. Defenses are improving, and campaigns are raising public awareness. Critically, collaboration is growing: not yet at scale, but plans are in the works, and localized initiatives have already recorded some successes. Stay tuned as the next chapter unfolds.

Glossary and Methodology

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, marketplaces, travel, 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 to access online services or obtain lines of credit.

Account Login Fraud: Attacks attempting to take over user accounts with stolen credentials either sourced in the wild or via 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 (for example account creations, account login and payments) from mobile devices and computers processed by our 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, depending 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 as defined above.

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 to change their device identity or fingerprint, or attempt to appear to come from a victim's device. Patented cookieless device identification from LexisNexis® ThreatMetrix® can 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, customize 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 elude 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 by our LexisNexis® Digital Identity Network® from Jan – Dec 2025, during near real-time analysis of consumer interactions across the online journey, from new account creations through logins, payments and other non-core transactions such as password resets and transfers.
- Transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioral analytics.
- Digital Identity Network® and its near real-time policy engine provide unique insight into global digital identities across applications, devices and networks.
- 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 U.S. and Canada. Mexico is included in the LATAM regional analysis.

DATA PROCESSED AND ANALYZED

The overall volume of transactions processed by our Digital Identity Network from Jan-Dec 2025 was 139 billion.

- The LexisNexis Cybercrime Report analyzes a subset of these transactions that excludes non-transaction-based events (such as feedback data and test transactions) and excludes transactions from organizations considered outliers based on extremely high or zero recorded reject rates. This subset totals 116 billion transactions.
- The Cybercrime Report uses these 116 billion transactions to calculate overall transaction volumes globally and by region. There are 3.8B transactions without an IP address. These transactions cannot, therefore, be assigned to a region. These are mostly unknown sessions where an organization does not send the input IP address.
- This subset of 116 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 on a further subset of 107 billion transactions. These are categorized 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 www.risk.lexisnexis.com and www.relx.com.