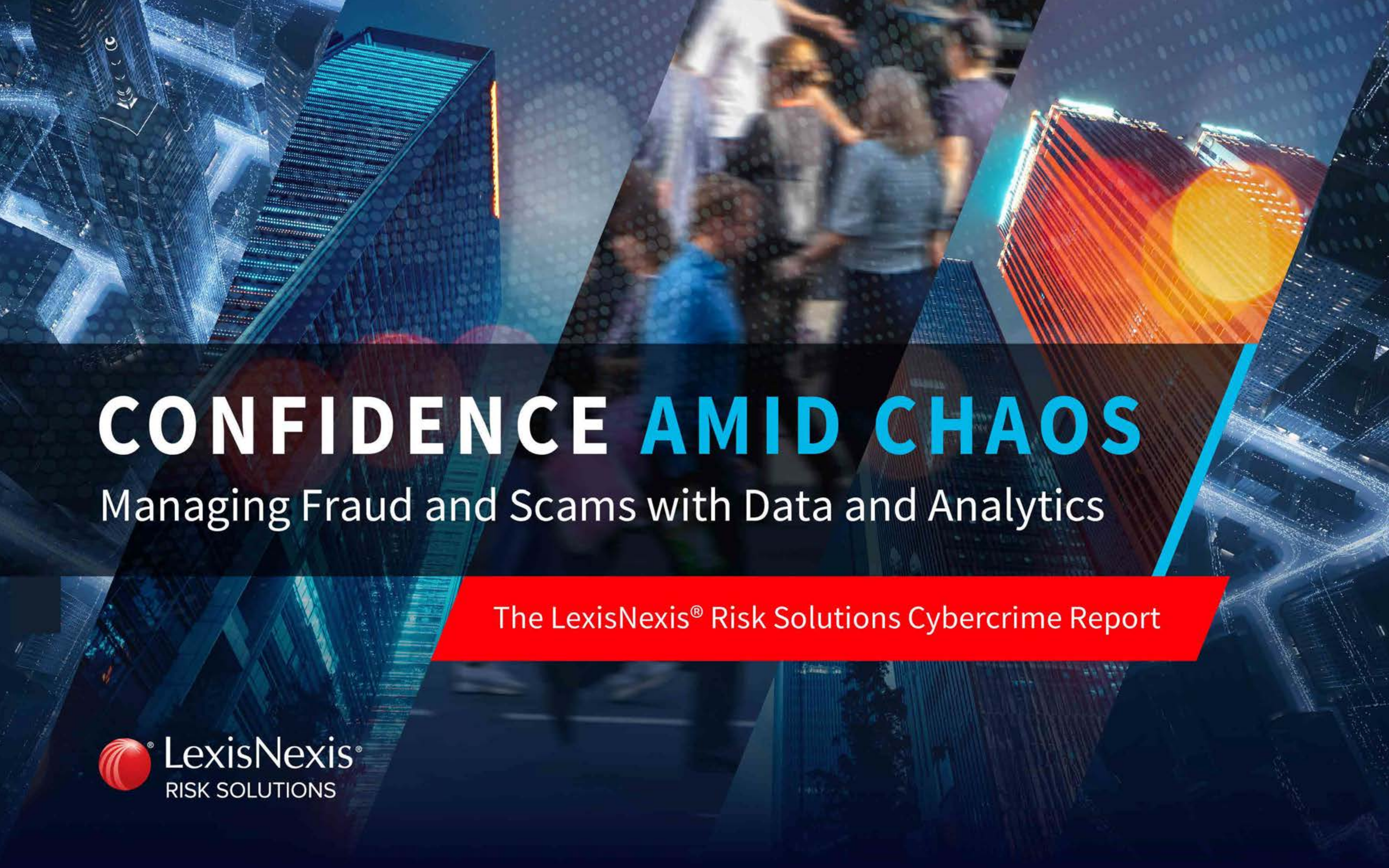


CONFIDENCE AMID CHAOS

Managing Fraud and Scams with Data and Analytics

The LexisNexis® Risk Solutions Cybercrime Report

LexisNexis®
RISK SOLUTIONS

INTRODUCTION

TABLE OF CONTENTS:

Introduction

Digital fraud attack rates recorded in the LexisNexis® Digital Identity Network® platform continued climbing in 2023, increasing 19% year-over-year, maintaining a trajectory first noted in the LexisNexis® Risk Solutions Cybercrime Report 2022. Organizations operating in North America (up 43% YOY) or in the ecommerce sector (up 59% YOY) sustained the greatest increase in fraud attack rates.

Gaming and gambling operators reported a 103% increase in bot volume, seemingly drawing bots away from other industries. Unsophisticated bots still serve a purpose, providing bad actors an efficient means to test data either for resale or direct attack. Bot traffic followed a surge of legitimate consumers flocking to gaming and gambling operators in multiple countries with modernizing regulations.

Fraud thrives in changing circumstance, such as the widespread and ongoing adoption of new technologies. The initial application of generative AI to fraud attacks in 2023 gives cause for concern now, but will likely be regarded as unsophisticated with the hindsight of a few more years' innovation. Take, for example, how fraudsters continue to hone their illicit exploitation of instant payment systems as a vehicle to target consumers via authorized payment fraud ("scams"). As more consumers adopt instant payments, and as more instant payments platforms enable international transfers, fraudsters will likely continue to exploit the payments channel.

Scams have grown into a pandemic, leading to significant regulatory activity around the world in 2023. Many regulators focused on operational or technical requirements to defend against scams, likely waiting to see the results of some countries' focus on liability and reimbursement, beginning with the UK. Collaboration is growing around the world, including regulated data-sharing initiatives in Brazil and Hong Kong, and collaborative consortiums beginning in the United Arab Emirates and in Singapore.

Every year, the LexisNexis® Risk Solutions Cybercrime Report illustrates the power of organizations collaborating across international and industry boundaries. Reports of confirmed and suspected fraud and abuse from seemingly unrelated corners of the global market help to improve all participants' confidence in clearing the path for trusted consumers and transactions. We thank the many organizations whose anonymized contributions provide the basis for this report, and for the tenacity to continue making our world a safer place, together.

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

- Networked fraud at global and regional levels
- Detecting sophisticated bot attacks
- Scam center signatures
- Mule account classifications

GLOBAL RISKS

JANUARY-DECEMBER 2023 ANALYSIS

Global Highlights: January-December 2023

Transactions

+15% ▲	Global transaction volume year-over-year (YOY)
+17% ▲	Financial services transactions
+7% ▲	Ecommerce transactions
-10% ▼	Communications, mobile and media (CMM) transactions
+66% ▲	Gaming and gambling transactions

Human-Initiated Attacks

+19% ▲	Human-initiated attack rate YOY
+8% ▲	Financial services attack rate
+59% ▲	Ecommerce attack rate
+11% ▲	Communications, mobile and media attack rate
-3% ▼	Gaming and gambling attack rate

Automated Bot Attacks

+2% ▲	Automated bot attacks YOY
-6% ▼	Financial services bot volume
+6% ▲	Ecommerce bot volume
-46% ▼	Communications, mobile and media bot volume
+103% ▲	Gaming and gambling bot volume

LexisNexis® RISK SOLUTIONS

Attacks noted by the Digital Identity Network® are split by human-initiated attacks, which typically return full digital identity profiling data relating to individual events, and high-velocity automated bot attacks.

Global Transaction Patterns in Numbers

Shift to Mobile Slows as Traditional Browser Traffic Lives On

Consumers continue to shift to mobile but at a slower rate. Mobile transactions, primarily on apps, increased 4% year-over-year. This may reflect a percentage of the population that is not moving to mobile, highlighting the need for organizations to offer multiple channels of engagement.

New account creation growth restarted in 2023 after showing little growth in 2022. As consumers became more comfortable logging into existing accounts and making digital payments, they seem ready to continue expanding their digital footprints.

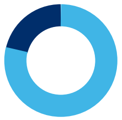
TRANSACTIONS ANALYZED

JANUARY-DECEMBER 2023

92.0B .... Growth YOY +15% ▲

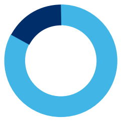
TRANSACTIONS BY CHANNEL

Desktop / Mobile



21% / 79% .... Growth YOY +4% ▲

Mobile Browser / Mobile App



17% / 83% .... Growth YOY +1% ▲

TRANSACTIONS BY USE CASE

New account creations, logins and payments are the three primary use cases analyzed. Further use cases are discussed later on in the customer journey section of the report.

		Growth YOY
New Account Creations	1.1B	+13% ▲
Logins	67.1B	+14% ▲
Payments	15.3B	+20% ▲

Global Attack Patterns in Numbers

Human-Initiated Attacks Proliferate While Bots Target Gamers and Gamblers

The overall attack rate continued a brisk pace of growth set in 2022, up 19% YOY at 1.5%. Ill-gotten funds fuel fraudsters' investments in capabilities to target more consumers and organizations, including more automation and AI/ML to improve operational versatility and efficiency.

The mobile browser channel bore the greatest attack rate growth, implicating the channel as the least secure. The lightweight nature of mobile browsers limits the availability of digital intelligence and risk signals, a boon to attackers relying on ambiguity. The preponderance of mobile app transactions makes that channel's comparatively muted attack rate growth more concerning for organizations meeting consumer demand for mobile experiences overall.

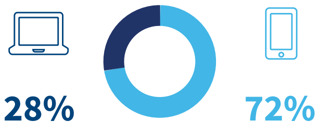
Automated bot attacks remained stable compared with last year, though the targets shifted. Gaming and gambling organizations saw a 100% increase in bot attacks in 2023 compared to 2022. Ecommerce bot attacks remain elevated after significant increases last year, signaling a possible new benchmark. Financial services continue to sustain the most attacks overall.

HUMAN-INITIATED ATTACKS

ATTACK VOLUME

	Growth YOY
1.3B	+40% ▲

Attack Volume by **Desktop** / **Mobile**



ATTACK RATE		Growth YOY
OVERALL	1.5%	+19% ▲
DESKTOP	2.0%	+19% ▲
MOBILE BROWSER	3.7%	+36% ▲
MOBILE APP	0.9%	+13% ▲

Percentage of attacks coming from mobile devices has **increased YOY** +5% ▲

AUTOMATED BOT ATTACKS

ATTACK VOLUME

	Growth YOY
3.6B	+2% ▲

		Change YOY
Financial Services	1.8B	-6% ▼
Ecommerce	1.5B	+6% ▲
Gaming and Gambling	201M	+103% ▲
CMM	25M	-46% ▼

LexisNexis® RISK SOLUTIONS

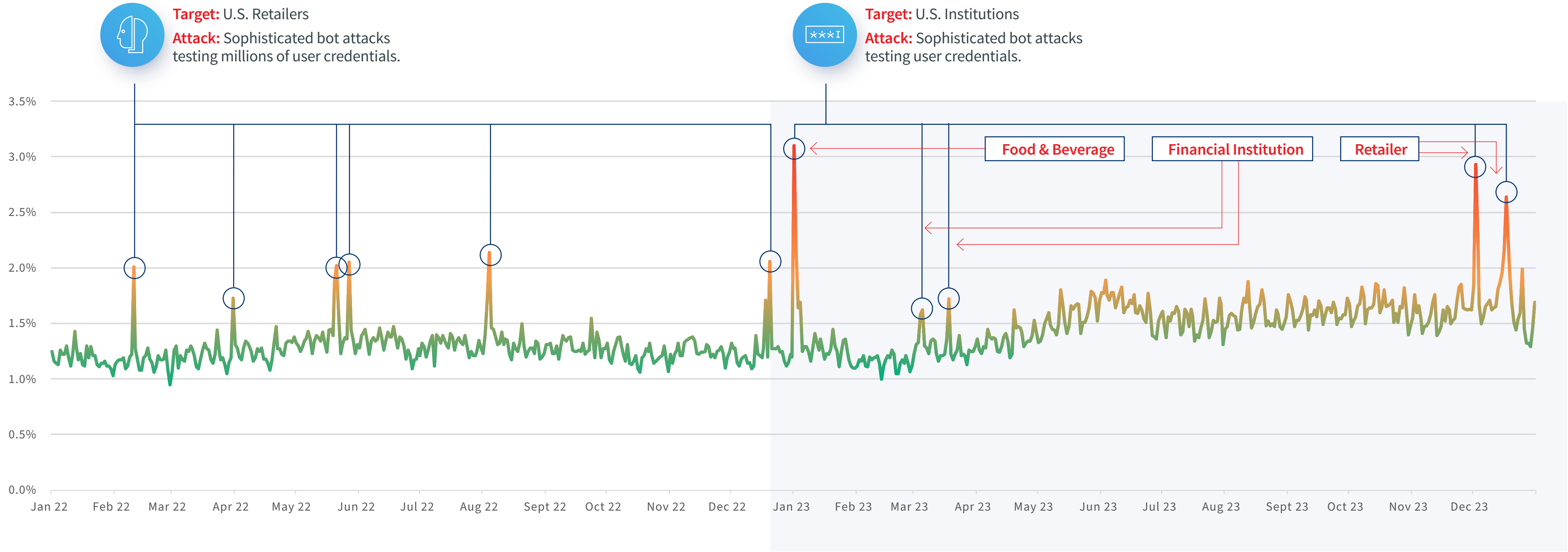
Identity Abuse Index

North America Drives the Global Index Higher

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day, across the entire Digital Identity Network. This includes human-initiated and sophisticated bot attacks. The identity abuse index grew 19% in 2023, following a similar (20%) increase in 2022. Fraudsters increase their attacks on potential victims, with North America contributing significantly to the global growth.

IDENTITY ABUSE INDEX

● LOW ● MEDIUM ● HIGH



Target: U.S. Retailers
Attack: Sophisticated bot attacks testing millions of user credentials.

Target: U.S. Institutions
Attack: Sophisticated bot attacks testing user credentials.

An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations from the medium-term trend.

Global Networked Account Takeover Fraud

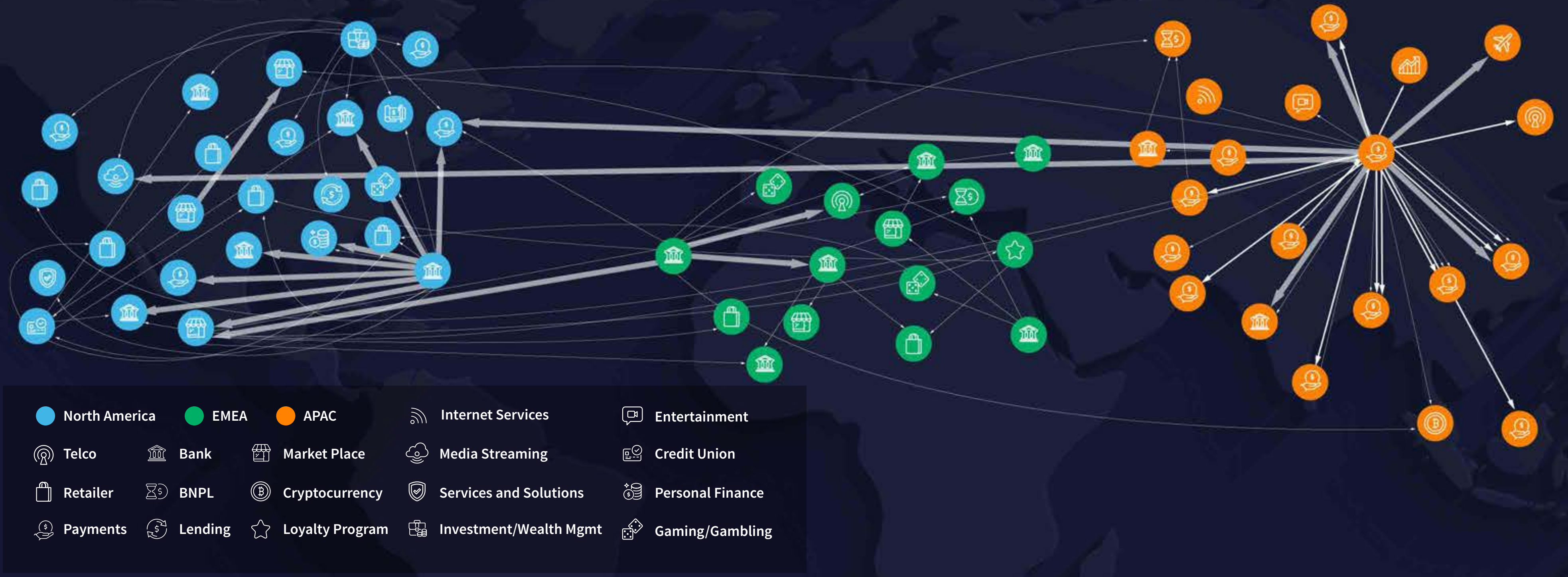
Fraudsters Share Compromised Credentials and Align on Phishing Scam Techniques

This diagram from Q4 2023 shows how bad actors indiscriminately target organizations across industries and borders.

Circles represent member organizations within the LexisNexis Digital Identity Network platform. Arrows represent digital identities, who have been associated with confirmed fraud at a source organization, attempting to interact or transact with a target organization. A thicker line denotes a higher volume of attacks.

97% of the events seen in this network are logins, with 3% payments, highlighting the need to monitor at login in addition to payment.

The diagram shows that whilst fraud rings may often work within geographical regions, there is generally evidence of collaboration across international regions. In this example Market Places and Payment Providers tend to draw the fraudsters cross-border or more specifically cross-region.



LexisNexis®
RISK SOLUTIONS

Fraud Types from a Client Perspective

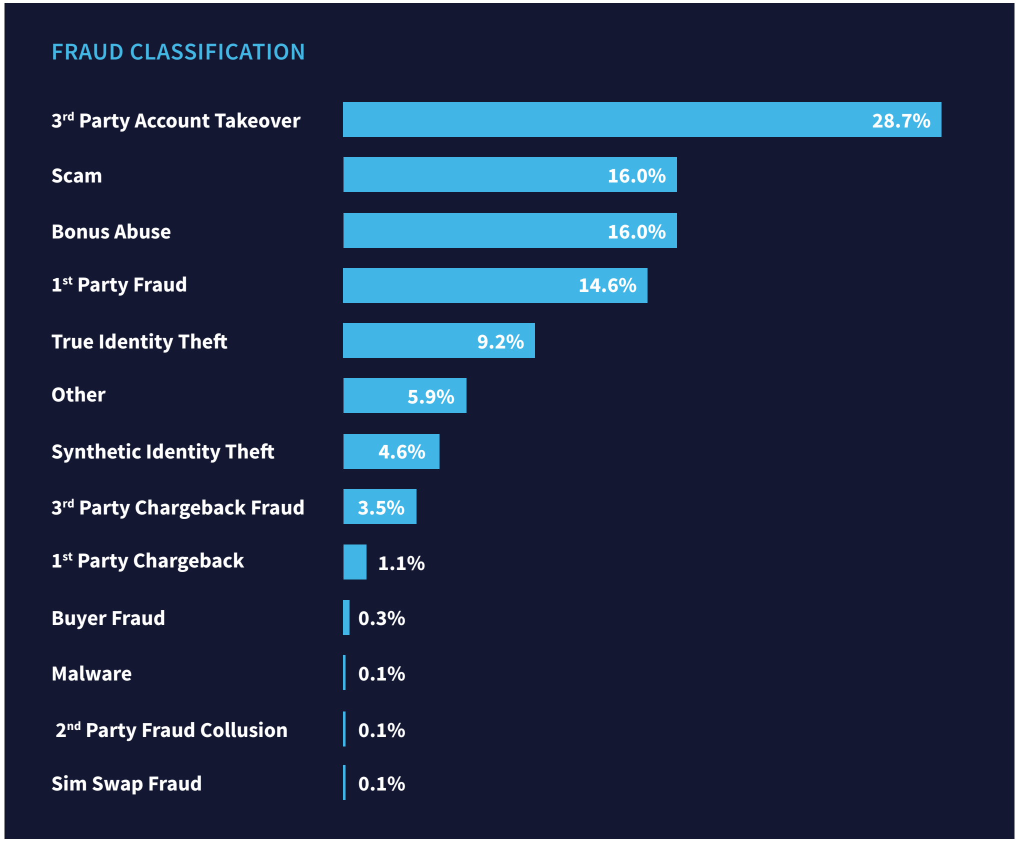
Focus on 3rd Party Account Takeover Grows

The chart on this page shows how fraud attempts in the Digital Identity Network platform are classified by our clients. The top four classifications in 2023 are third-party account takeover, bonus abuse, first-party fraud and scams.

The classifications overlap somewhat due to client interpretations and differing terminologies around the world. For example, third-party account takeover may be the result of authentication data compromised as part of a phishing or social engineering scam. A client may classify such a scenario as either a scam or an account takeover.

Third-party account takeover as a percentage of all classifications grew strongly in 2023 to take the top spot. This aligns with the strong attack rate growth seen at login in 2023 (up 18% YOY).

The complexity, variability and increasing sophistication of fraud demands organizations maintain robust systems composed of multiple, targeted fraud detection models. Complementary models are more capable than singular models of assessing risk in near real time and seeking anomalies associated with different types of attacks. To maintain efficacy, fraud models require classified fraud feedback data from historic events, with classifications based on context and modus operandi.



Fraud Classifications by Region and Industry

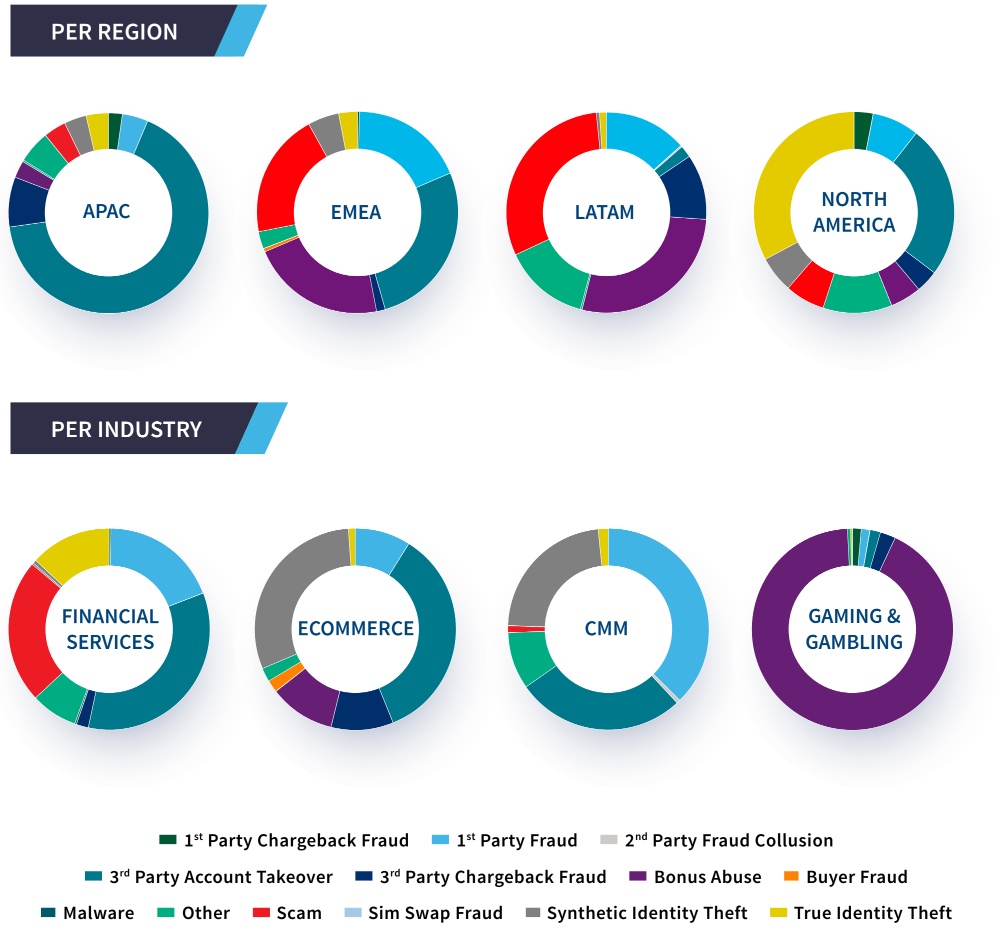
Account Takeover and Bonus Abuse Proliferate

Fraud classifications vary significantly between regions and industries due to combinations of local idiosyncrasies, but also nuanced differences in definitions and interpretations of fraud types (for example, scams).

In APAC third-party account takeover has become even more dominant than in 2022, driven by a relentless scam pandemic across the region which for now is primarily fueling subsequent unauthorized fraud attempts, in contrast with the authorized transfer scams seen in EMEA. Bonus abuse worsened in both EMEA and LATAM, linked to both gaming and gambling and ecommerce. North America saw significant YOY percentage growth of true identity theft in 2023, offsetting a decline in third-party chargeback fraud as a percentage of all classifications.

Third party account takeover and synthetic identity theft become more important concerns for CMM in 2023, significantly reducing the prominence of first-party fraud compared to 2022. Account takeover fraud as a percentage of the total classifications grew strongly for both ecommerce and finance in 2023.

Bonus abuse dominated all other fraud classifications for gaming and gambling in 2023. The online industry's growth around the globe affords fraudsters more opportunity to hide among the surge of new digital players legitimately acquiring sign-up bonuses.



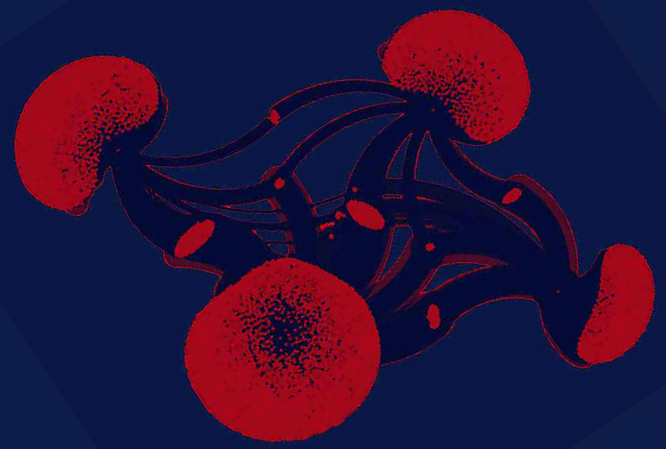
Bot Sophistication Grows

Over 3.5 billion bot attacks were identified in the Digital Identity Network in 2023. Financial services organizations bore half of these attacks, with ecommerce sustaining most of the rest. Gaming and gambling operators saw a 103% increase in bot attacks.

Bots are not new; however, their automated capabilities and sophistication continue to increase. Traditional bot prevention solutions often focus only on large-scale bot attacks, but fail to detect more advanced bots that exhibit more human-like behavior as an evasion tactic. Detecting advanced bots in near real time can greatly mitigate their ability to create fraudulent accounts or test login credentials for subsequent account takeover attacks.

Advanced bot detection capabilities can monitor for:

- Bot traffic that mimics the locations of good customers via IP proxies
- Abnormal timing of events as well as unusual on-page or in-app behaviors
- Evidence of the use of virtual machines to mimic real customer devices



In the example above, proxy piercing technology resolves thousands of proxy IP addresses down to four primary IP addresses. Proxy IPs can help to promote privacy, which makes them an appealing obfuscation tool for bad actors.

Scams and Scam Centers

The rapid rise in authorized payment fraud (known as Authorized Push Payment or APP fraud internationally and authorized transfer scams in the U.S.) has gone hand in hand with the growth of scam centers, such as those in mountainous, border regions in parts of South-East Asia. Media reports describe organized enterprises, with technical expertise to develop phishing sites and mobile malware as well as call centers, staffed by captive operators speaking multiple languages.[1] Human trafficking groups supply the call centers with workers often held against their will.

These scam centers appear in data from the Digital Identity Network platform, such as a clear increase in high-risk digital events coming from border areas in Cambodia and Myanmar, and in high-altitude behavioral biometrics telemetry.[2]

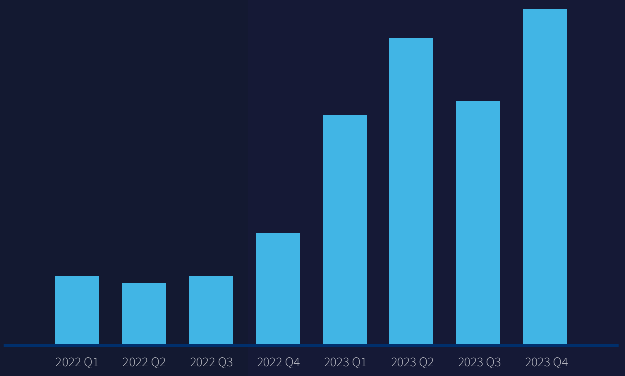
Fraudulent payments may be directly linked to scam centers in the case of unauthorized payment scams – such as when the scam involves the victim divulging their account authentication details under false pretense. More subtle evidence may be found in account access or mule account management (but not linked to payments themselves) when the focus is on authorized push payment scams, such as romance or investment scams.

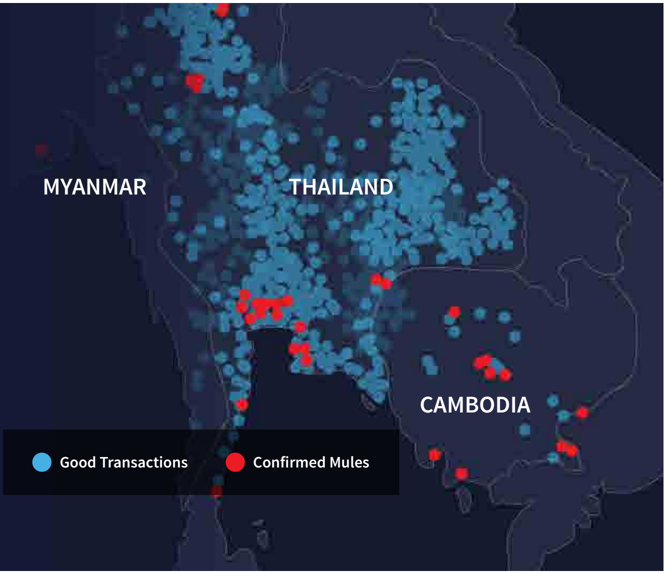
Advanced fraud detection models can help to identify signals from scam centers:

- Location data originating from high-risk areas
- Altitude data complementing location data when relevant
- Lack of natural movement, such as multiple devices at rest on a table

Fraud attempts are on the rise in Cambodia and bordering countries

CONFIRMED FRAUD ATTEMPTS FROM CAMBODIA





[1] Selected sources: www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report, www.japantimes.co.jp/news/2024/03/04/asia-pacific/crime-legal/thailand-scam-victims-myanmar-china/, www.voanews.com/a/scam-victims-say-human-trafficking-still-a-problem-in-cambodia/7520511.html, www.bbc.com/news/world-asia-68562643.amp
[2] risk.lexisnexis.com/insights-resources/article/mules-mobile-and-money-combatting-human-trafficking-fueled-fraud

Mule Account Classifications

Mule accounts are an integral part of the scam pandemic, facilitating money movement out of victims' accounts. This is in addition to their well-established role in money laundering and other financial crime.

Identifying mule accounts can help to improve a financial organization's scam prevention capabilities, with this intelligence feeding fraud models in real time.

A robust mule detection strategy must operate across the customer journey – not just at the moment of new account creation, but also at login and payment. Different types of mules exhibit different behaviors at different stages of the customer journey:

- Complicit mule accounts are created specifically for mule activity
- Witting mule accounts belong to owners who knowingly engage in mule activity
- Unwitting mule accounts belong to owners who unwittingly participate in mule activity (typically 10%-30% of mule accounts at a bank)

Machine Learning models operating on data from the Digital Identity Network can discern mule types by focusing on key metrics such as account age and account activity, alongside other digital identity attributes.

Identifying mule accounts enables scam mitigation at the moment of payment. Classification of mule accounts enables proactive management of the accounts themselves. Complicit mule accounts can be closed quickly. Unwitting mules can be alerted to the nefarious actions occurring via their accounts.

In 2023 the number of banks using the Digital Identity Network for mule account tracking, in addition to traditional fraud prevention capabilities, grew by 53% YOY, while the number of confirmed mules in the network grew by 64% YOY.

	ACCOUNT AGE	
ACTIVE ACCOUNT	NEW	EXISTING
INACTIVE	Complicit Inactive	Witting
ACTIVE	Complicit Active	Unwitting

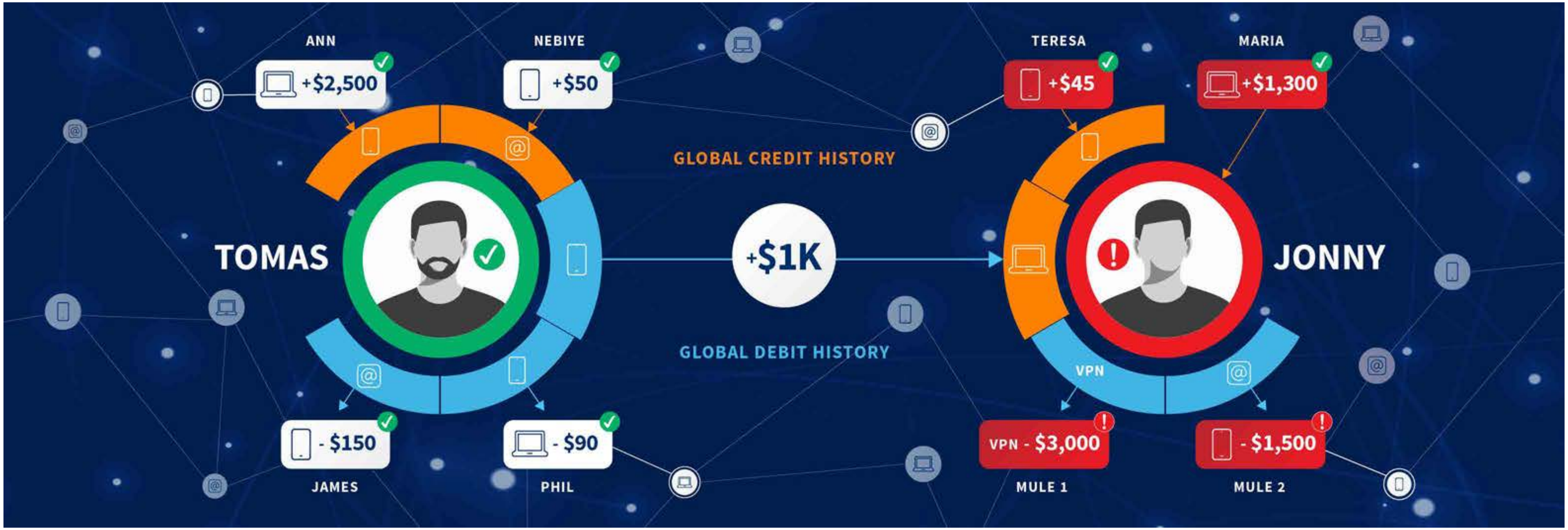
Mules can be classified based on activity and account age. Complicit mule accounts are set up and used for a short period of time or continue to be actively used until closed. Existing accounts may become involved knowingly or unwittingly in mule activity – their regular behavior may change, identifying whether they are complicit or not.

Determining Risk Associated With Beneficiary Accounts

Due to the surge of authorized push payment scams, and prospective regulatory action, financial institutions and payment service providers face an increasingly likely future where they will need to assess beneficiary risk before completing transfers requested by consumers.

To help improve scam detection and mitigation, as well as to identify money mule accounts more effectively, successful payment defense models integrate data about payee identities and accounts, beneficiary identities and accounts and transaction risk. The most powerful models add the further dimension of digital identity intelligence – linking transactions through multiple network layers, rather than just payment flows alone.

Models optimized via machine learning dynamically determine risk associated with beneficiary accounts based on historic and real-time trends. For example, during one month in 2023 more than 30% of the consumer-initiated payments to one digital bank in the UK were identified as fraudulent via this technique.



ACROSS THE CUSTOMER JOURNEY

JANUARY-DECEMBER 2023 ANALYSIS

Customer Journey Highlights: January-December 2023

New Account Creations

1 in every 11 new account creations are attacks

CMM has highest industry attack rate **at 12%**

345% YOY growth in gaming & gambling new account creation bot attacks

Logins

0.8% attack rate **(18% growth YOY)**

119% YOY growth in ecommerce login attack rate

Password Resets

135% YOY growth in attack rate

1 in 5 password reset attempts through desktop browsers are attacks

870% growth in bot attacks on password resets

Detail Changes

232% YOY increase in attacks

1 in 10 details change attempts via mobile browsers were attacks

61% growth in bot attacks via detail changes

Payments

Highest mobile share of transactions **(80% of payments are mobile)**

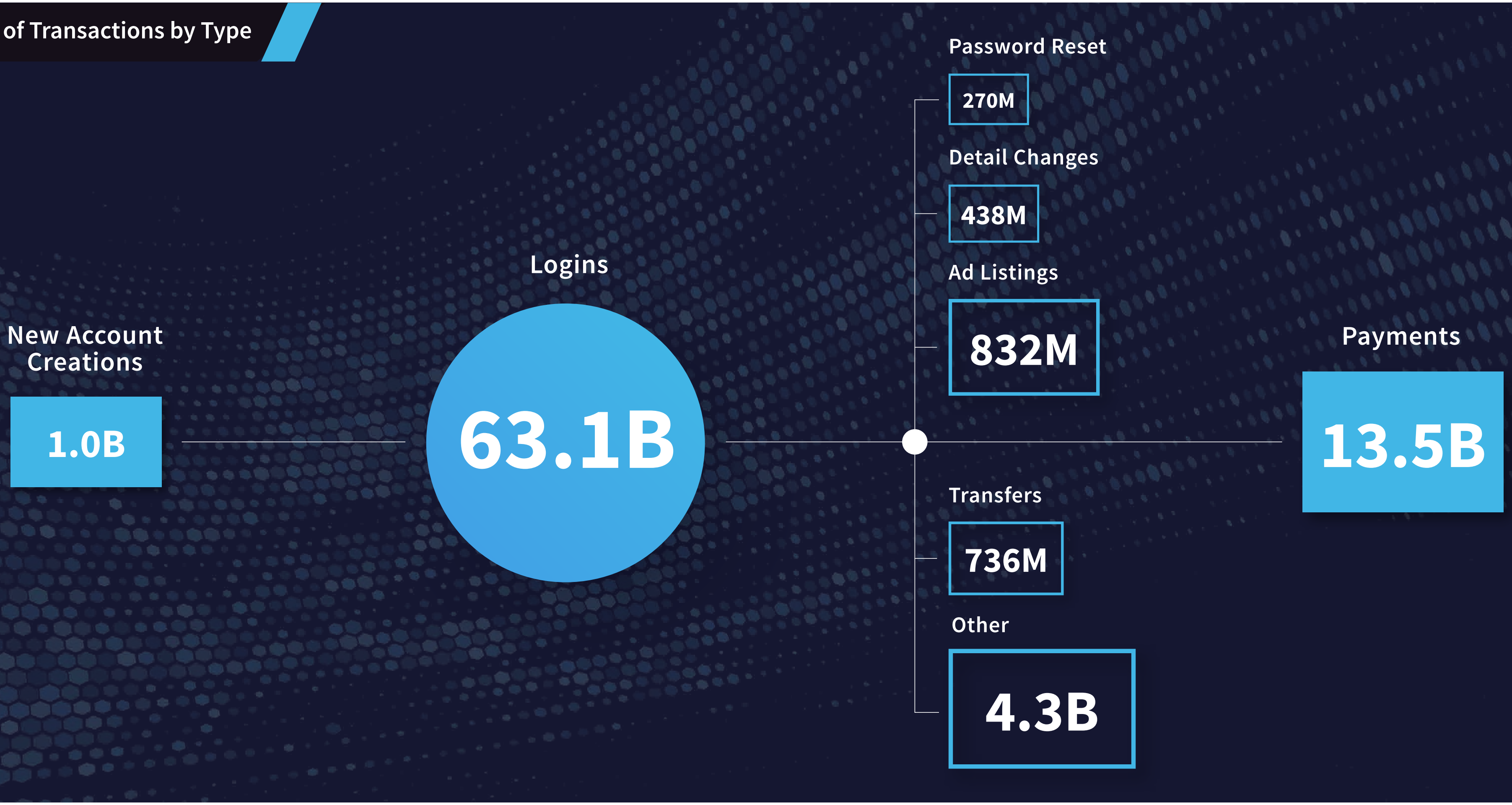
Most frequently attacked use case **by volume**

LexisNexis® RISK SOLUTIONS

Volume of Transactions by Use Case Across the Online Journey

Profiling Risk Across Each Customer Touch Point

Volume of Transactions by Type



Password Reset

270M

Detail Changes

438M

Ad Listings

832M

Logins

63.1B

New Account Creations

1.0B

Payments

13.5B

Transfers

736M

Other

4.3B

LexisNexis® RISK SOLUTIONS

Transaction volume by use case is calculated using a subset of the total transaction volume, where outliers and unknown sessions are removed.
Transaction "other" includes: New Device Registration, Digital Download, Account Balance, Loan Acceptance, Auction Bid and more.

Attack Risks Across Core Touchpoints

Account Takeover and Payment Fraud Risk Continues to Grow

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account creations continue to be one of the highest risk touch points in the customer lifecycle – second only to password reset risk in 2023. New sign-ups through browser channels are significantly more risky than via mobile app.	Cybercriminals continue to focus on account takeover attacks, driving an 18% YOY increase in 2023 after a 52% YOY increase in 2022. Ecommerce accounts sustained much of the attack growth.	The payment attack rate grew by 13% YOY following the general trend upwards. Attacks via the mobile app increased more than other channels, up 27% YOY.
ATTACK RATE			
OVERALL	9.2%	0.8%	4.2%
DESKTOP	**11.6%**	1.3%	4.0%
MOBILE BROWSER	10.1%	**2.0%**	**5.0%**
MOBILE APP	3.7%	0.5%	3.6%

LexisNexis® RISK SOLUTIONS

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 More High-Risk Touchpoints

To Complete an Account Takeover Attack, Fraudsters Change Contact Details and Passwords

	PASSWORD RESETS	DETAIL CHANGES	AD LISTINGS	TRANSFERS	OTHER
RISK TRENDS	Consistently identified as a high-risk touchpoint, password reset attacks grew by 135% YOY. Current attack trends favor the desktop browser channel, with the attack rate via mobile app having decreased by 74% YOY.	The greatest YOY increase in attacks (232%), details change touchpoints hold great value for fraudsters. When user authentication occurs solely at login, details change touchpoints conclude account takeover attacks.	Overall attack rates for ad listings declined slightly in 2023. Ad listings allow fraudsters to control the sale or promotion of goods and services, provide a way of monetizing stolen goods, or creating phony reviews to facilitate sales.	Attack rates associated with transfers declined slightly in 2023. Transfers move money into a different account within a customer's overall profile, an action that can precede a fraudulent payment event.	Encompassing several other high-risk touchpoints, such as new channel registration, standing order mandates, direct debits and beneficiary modifications. Attack rates associated with other touchpoints rose 24% YOY.
ATTACK RATE					
⚠ OVERALL	13.7%	3.8%	0.4%	0.7%	1.3%
DESKTOP	**23.1%**	4.0%	**0.8%**	**1.1%**	1.3%
MOBILE BROWSER	2.4%	**10.0%**	0.7%	0.8%	**1.9%**
MOBILE APP	1.8%	0.9%	0.3%	0.7%	1.0%

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

JANUARY-DECEMBER 2023 ANALYSIS

Regional Highlights: January-December 2023

APAC

+20% ▲ transaction volume YOY

-5% ▼ human-initiated attacks YOY

-12% ▼ bot volume YOY

EMEA

+20% ▲ transaction volume YOY

+28% ▲ human-initiated attacks YOY

+9% ▲ bot volume YOY

LATAM

+15% ▲ transaction volume YOY

+20% ▲ human-initiated attacks YOY

+35% ▲ bot volume YOY

North America

+12% ▲ transaction volume YOY

+66% ▲ human-initiated attacks YOY

-4% ▼ bot volume YOY

North America includes the U.S. and Canada. Mexico is included in the LATAM regional analysis.

Identity Abuse Index by Region

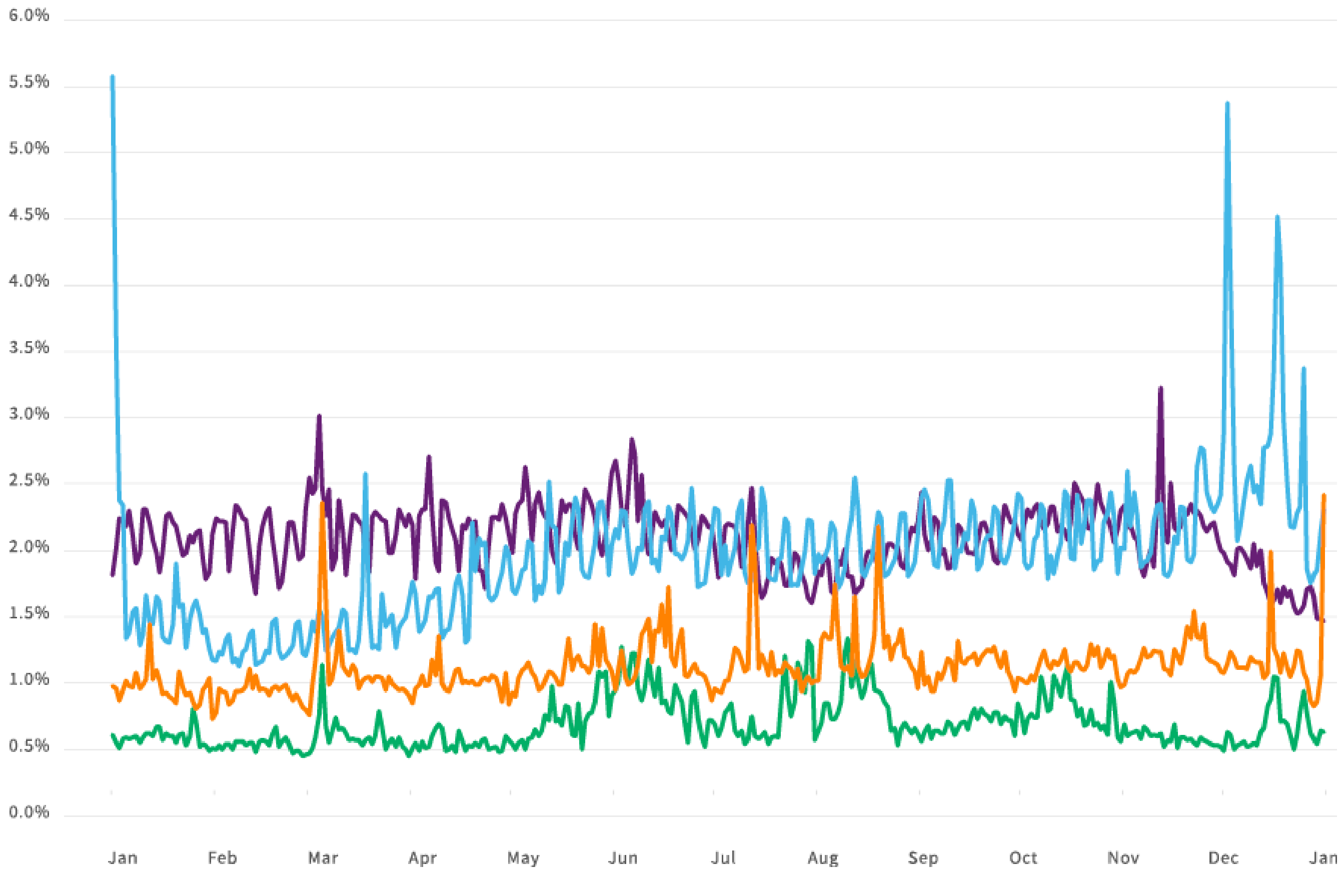
Attack Rate in North America Surges as Ecommerce is Targeted

● **APAC** attack rate on average declined in 2023 compared with 2022. The region's annual attack rate for 2023 remained below that of North America, in contrast with 2022.

● **EMEA** retains the lowest regional attack rate, despite elevated attacks in June and August.

● **LATAM** endured an elevated and persistent rate of attack throughout the year, as in 2022. An end-of-year dip tempered an otherwise sustained high among the regions.

● **North America** attack rate grew significantly during 2023, with major attacks during the holiday season.



LexisNexis®
RISK SOLUTIONS

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day, across the entire Digital Identity Network. This includes human-initiated and sophisticated bot attacks.

APAC: Transaction and Attack Patterns

ATTACK SPOTLIGHT

JANUARY-DECEMBER 2023

- Targeted bot attacks in May on Australian telcos originating from Finland, the U.S., China and Germany.
- Elevated attack rates from Malaysia and Cambodia on APAC organizations.

TRANSACTIONS

TRANSACTIONS ANALYZED

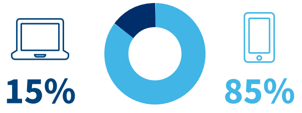
8.5B

Growth YOY

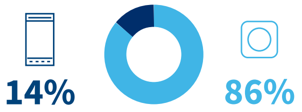
+20% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**



Mobile Browser / **Mobile App**



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

89M

Decline YOY

-5% ▼

AUTOMATED BOT ATTACK VOLUME

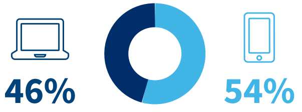
398M

Decline YOY

-12% ▼

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**



Percentage of attacks coming from mobile devices has **increased YOY**

+6% ▲

LexisNexis® RISK SOLUTIONS

APAC

Regulation and Technology Supporting the Fight against Scams

Regulators and financial institutions across the region worked diligently to respond to the significant growth in digital fraud sustained in 2022.

In an effort to clamp down on malicious text messages, organizations using SMS/text-based One-Time Passwords (OTP) were required to register with an SMS Sender ID Registry.

In response to more advanced mobile malware, public awareness campaigns warned consumers never to access links sent in messages, and to install apps only via the official app stores.

Banks have enhanced capabilities to detect and stop unauthorized fraud, primarily, leaving authorized push payment scams a vulnerability for consumers in the region generally.

These measures likely helped to set the APAC attack rate on a downward trajectory in a year when the global average attack rate grew.

Looking ahead to 2024, the expansion of cross-border instant payment schemes (for example: Thailand, Singapore, Malaysia and India), and the ease of targeting consumers directly via scams, will inevitably attract fraudsters.

ATTACK RATES 🌐 GLOBAL 📍 APAC

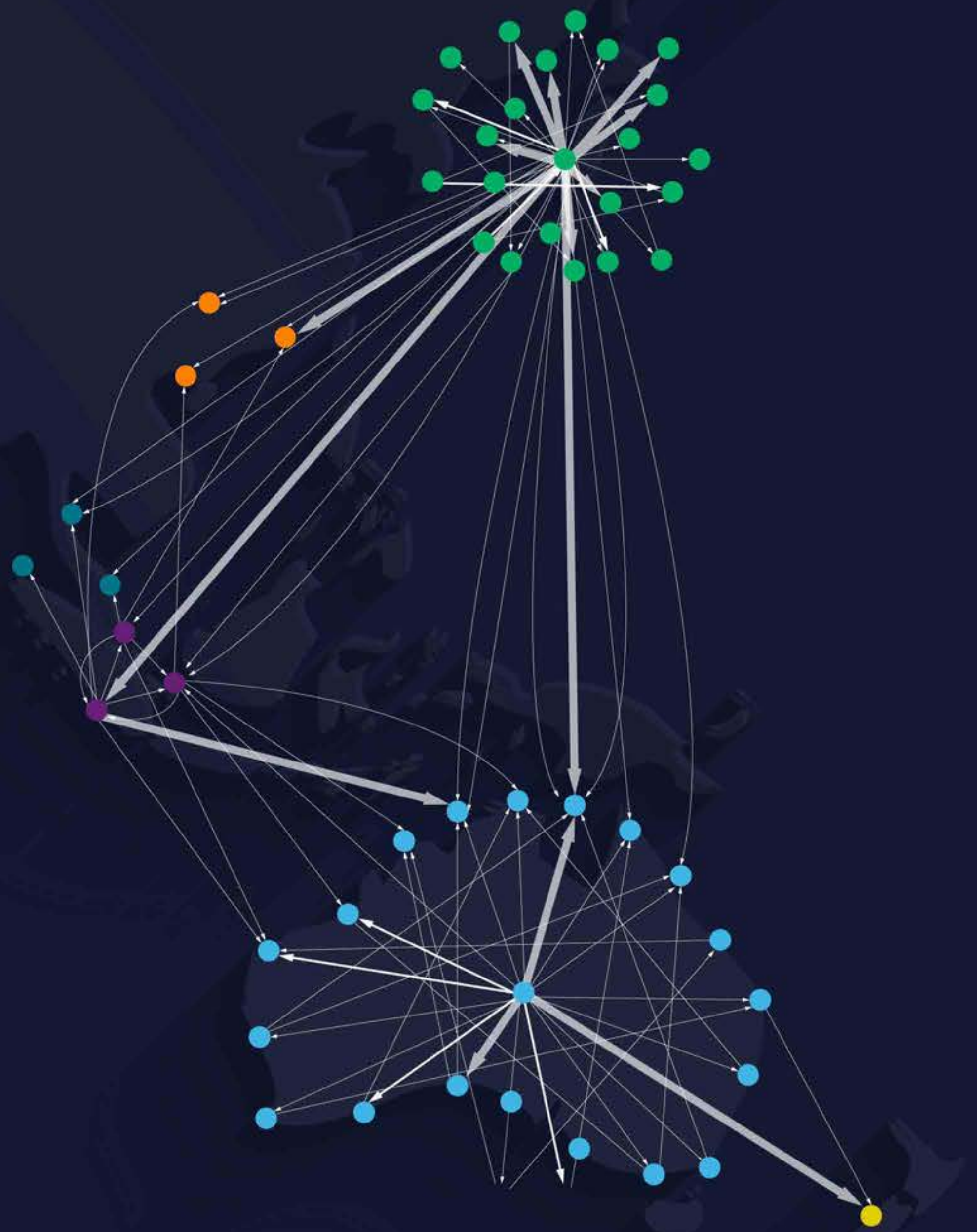
	🌐	📍
OVERALL	1.5%	1.1%
DESKTOP	2.0%	3.5%
MOBILE BROWSER	3.7%	3.5%
MOBILE APP	0.9%	0.3%

APAC Networked Fraud

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in APAC during the last quarter of 2023.

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

The diagram shows the cross-border nature of fraud within parts of East and South-East Asia, while highlighting more insular focused fraud rings operating in Australia and Japan. Of the events represented in this visualization, 69% occurred at payment and 26% occurred at login.



🔵 Australia	🟠 Hong Kong	🟢 Japan
● Malaysia	🟡 New Zealand	🟣 Singapore

EMEA: Transaction and Attack Patterns

ATTACK SPOTLIGHT

JANUARY-DECEMBER 2023

- Growth in ticket upgrade fraud spurred airlines to leverage digital intelligence for more confidence in consumer identity.
- Bot attacks on gaming and gambling operators in February and July contributed to a 103% increase in attacks year-over-year.

TRANSACTIONS

TRANSACTIONS ANALYZED

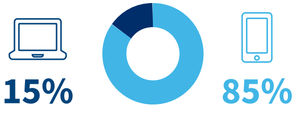
28.5B

Growth YOY

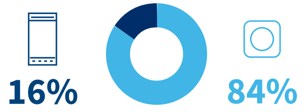
+20% ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

181M

Growth YOY

+28% ▲

AUTOMATED BOT ATTACK VOLUME

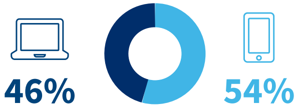
1.1B

Growth YOY

+9% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / Mobile



Percentage of attacks coming from mobile devices has **decreased YOY**

-6% ▼

EMEA

Managing Increased Scam Complexity while Preparing for Liability Frameworks

Fairly stable attack rates in EMEA obscures an on-going battle between fraudsters and organizations offering digital services to their customers. As the general public becomes more aware and suspicious of scams, fraudsters develop more complex attacks and convincing narratives, innovating with automation and Generative AI tools. Relentless persistence of scammers compels banks to integrate consistent prevention measures across channels.

In the UK, regulation activating in 2024 will define a clear liability framework for banks and spur greater collaboration within the industry. Implementation may take time, but the end result should provide consumers with some reassurance. Continental Europe looks on and adjusts its PSD3 draft framework accordingly.

Conversely, in Africa and the Middle East, scam activity is surging. In the Middle East, scammers exploit disruption caused by ongoing digitization of services, and target groups that are relatively new to the area, such as expat and transient populations. It's a similar story in Africa, where scammers abuse the ongoing roll-out of faster and alternative payment methods to target consumers, especially younger populations. The dynamism in these regions may also be inadvertently fueling substantial increases in account takeover attacks and synthetic identity fraud, in addition to scams.

ATTACK RATES

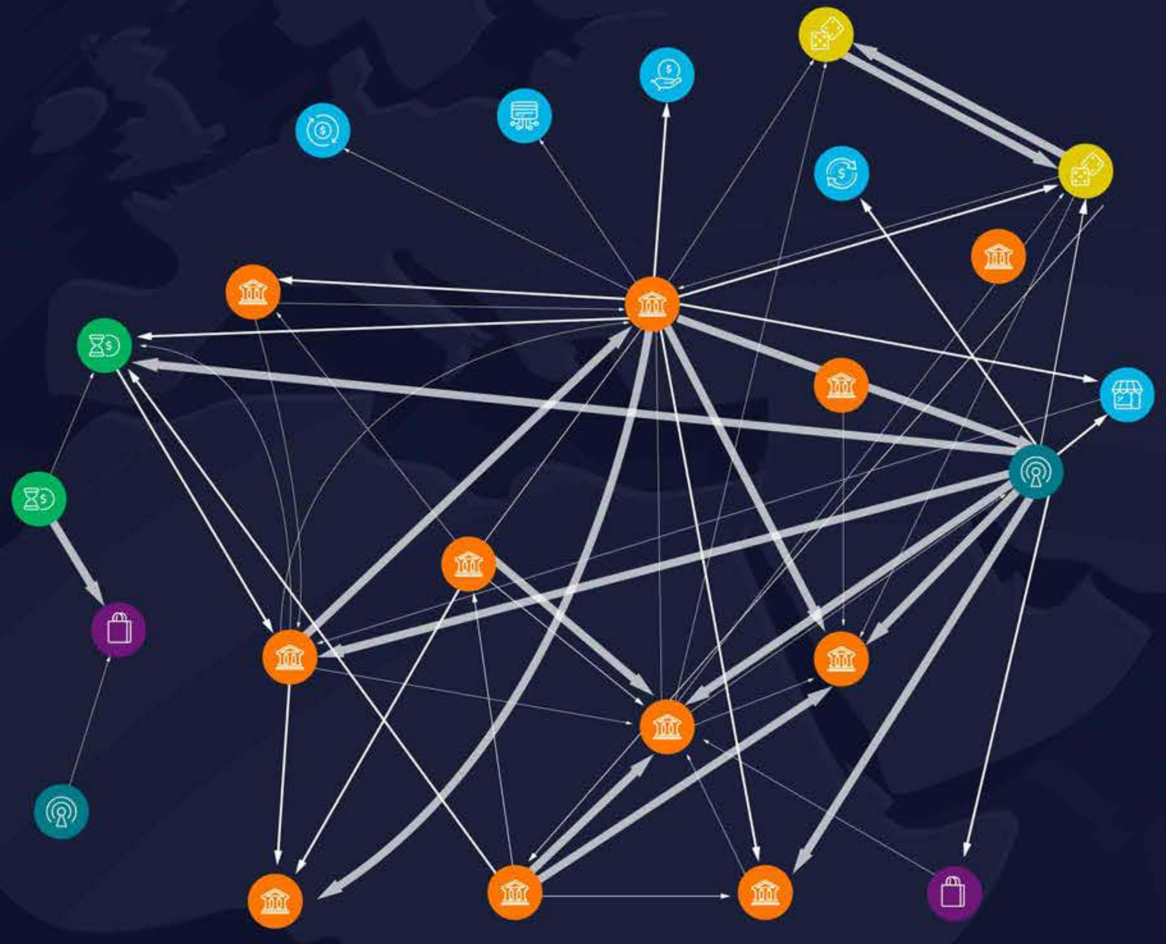
	GLOBAL	EMEA
OVERALL	1.5%	0.7%
DESKTOP	2.0%	2.1%
MOBILE BROWSER	3.7%	2.0%
MOBILE APP	0.9%	0.1%

EMEA Networked Fraud

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in EMEA during the last quarter of 2023.

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

The diagram illustrates how organizations can unite against fraud via digital identity, no matter the industry or geography.



● Bank	● Retailer	● Other	Market Place
● BNPL	● Telco	Card Network	Payments
● Gaming/Gambling		Lending	Remittance

LexisNexis®
RISK SOLUTIONS

LATAM: Transaction and Attack Patterns

ATTACK SPOTLIGHT

JANUARY-DECEMBER 2023

- The new account creation attack rate in LATAM grew more than twice as fast for digital banks than for all the region's financial institutions in 2023.
- Most human-initiated attacks on LATAM organizations in 2023 originated from Brazil, the U.S. and Mexico.

TRANSACTIONS

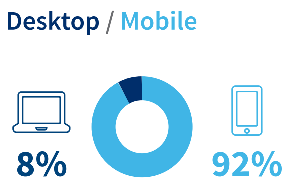
TRANSACTIONS ANALYZED

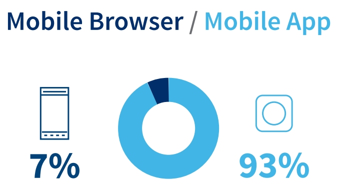
13.7B

Growth YOY

+15% ▲

TRANSACTIONS BY CHANNEL





ATTACKS

HUMAN-INITIATED ATTACK VOLUME

287M

Growth YOY

+20% ▲

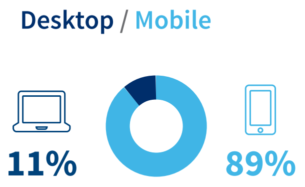
AUTOMATED BOT ATTACK VOLUME

376M

Growth YOY

+35% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL



Percentage of attacks coming from mobile devices has **not changed YOY**

0%

LATAM

App-First Posture Intended for Consumer Appetite Feeds Fraudsters

Digital transactions in LATAM grew at a slower pace compared to previous years as the region entered an economic downturn in 2023.

Consumers in the region continue to lead the globe in mobile app-based transactions, driven by strong growth with app-based services like PIX payments in Brazil. Attack rates likewise persisted above the global average, despite remaining relatively stable through 2023.

The new regulated digital gaming industry emerging across parts of LATAM (e.g. the Brazilian president signed a new Bill endorsing a legislative framework for online casino games on December 30th 2023) will inevitably become a target for attacks in 2024, given the attack volume the industry sustained elsewhere in 2023.

ATTACK RATES

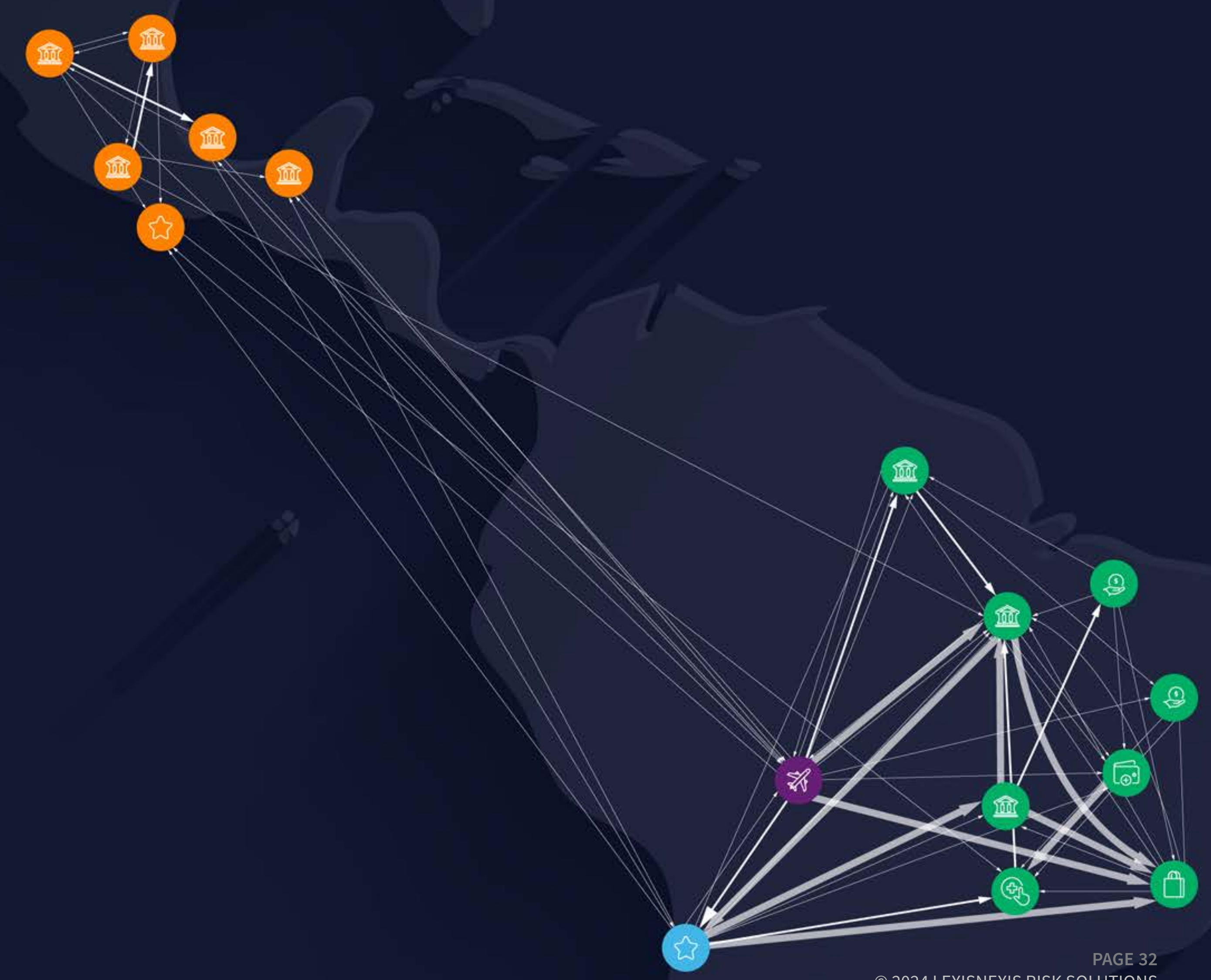
ATTACK RATES	GLOBAL	LATAM
OVERALL	1.5%	2.1%
DESKTOP	2.0%	2.9%
MOBILE BROWSER	3.7%	5.4%
MOBILE APP	0.9%	1.8%

LATAM Networked Fraud

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in LATAM during the last quarter of 2023.

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

The diagram shows fraud networks very much focused at the country level in Brazil and Mexico with little cross-border overlap between financial institutions. Perhaps unsurprisingly, the fraud network overlap is concentrated around travel-based organizations servicing multiple countries. Of the events represented in this visualization, 98% occurred at login, 1% occurred at payment with a further 1% at account creation.



● Argentina	● Brazil	● Chile	● Mexico
🏛 Bank	☆ Loyalty Program	✈ Travel	
Digital Wallet	Payments		
Insurance	Retailer		

LexisNexis® RISK SOLUTIONS

North America: Transaction and Attack Patterns

ATTACK SPOTLIGHT

JANUARY-DECEMBER 2023

- Significant credential-stuffing, password-reset and details changes attacks on ecommerce organizations in January and December.
- High payment attack rates from Vietnam, Mexico and China on ecommerce firms.

TRANSACTIONS

TRANSACTIONS ANALYZED

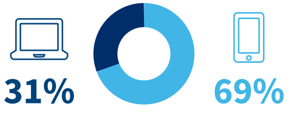
38.4B

Growth YOY

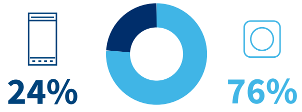
+12% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**



Mobile Browser / **Mobile App**



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

692M

Growth YOY

+66% ▲

AUTOMATED BOT ATTACK VOLUME

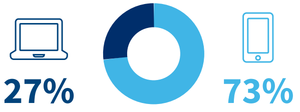
1.7B

Decline YOY

-4% ▼

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**



Percentage of attacks coming from mobile devices has **increased YOY**

+11% ▲

LexisNexis® RISK SOLUTIONS

North America

Human Attackers Swarm on the Mobile Channel, Hammer Ecommerce for Year-End Holidays

North America's attack rate grew sharply in 2023, for a second year, driven by a 66% YOY growth in human-initiated attacks. The bot attack rate remained stable after increasing substantially in 2022.

North America remains an attractive target for international fraud rings. The mobile channel is attracting more fraudsters, illustrating the need to maintain strong fraud prevention strategies on every channel.

The mobile app attack rate grew 47% YOY to 1.3%, with similar growth (63% YOY) driving the mobile browser attack rate to 4.5%.

Faster payments are gaining momentum in the United states, while Canada awaits the launch of Real-Time-Rail (RTR). Faster payments bring speed and convenience to payments, but also compel businesses to ensure they have effective solutions to curb fraud and safeguard their customers.

ATTACK RATES

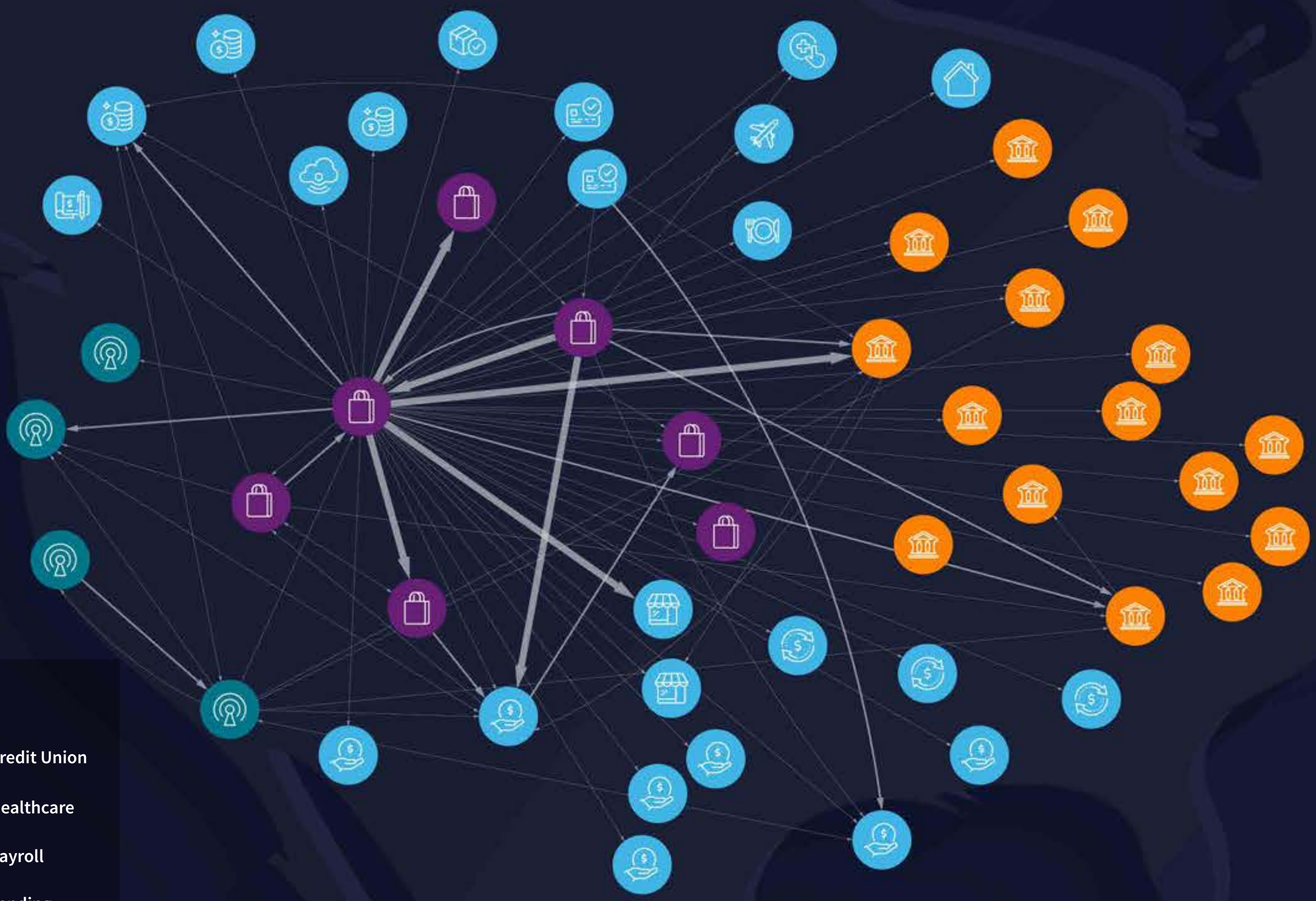
	GLOBAL	NORTH AMERICA
OVERALL	1.5%	1.9%
DESKTOP	2.0%	1.7%
MOBILE BROWSER	3.7%	4.5%
MOBILE APP	0.9%	1.3%

North America Networked Fraud

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in North America during the last quarter of 2023.

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

The diagram shows how digital fraud at the main North American retailers is tightly linked to the financial, CMM and payments industry.



● Bank	● Other		
● Retailer	Payments	Food	Credit Union
● Telco	Market Place	Real Estate	Healthcare
	Logistics/Mail Delivery	Personal Finance	Payroll
	Travel	Media Streaming	Lending

LexisNexis®
RISK SOLUTIONS

INDUSTRY OPPORTUNITIES

JANUARY-DECEMBER 2023 ANALYSIS

Industry Overview: Trends and Attack Patterns

Significant Growth of Attacks at Ecommerce Merchants Drives Attack Rates Higher

INDUSTRY OVERVIEW	ALL INDUSTRY SUMMARY	FINANCIAL SERVICES	ECOMMERCE	COMMUNICATIONS, MOBILE AND MEDIA	GAMING AND GAMBLING
RISK TRENDS	A 19% increase in the overall human-initiated attack rate YOY, with especially high growth in ecommerce.	Financial services firms sustained more attacks in 2023, but the overall attack rate increased at a slower pace than other industries.	The attack rate for ecommerce firms grew far more (59% YOY) than in any other industry, in both mobile and desktop channels.	The CMM industry attack rate grew at 11%, maintaining the highest overall attack rate of any industry.	The gaming and gambling attack rate remained stable in 2023, slightly down for the desktop channel. Bot attacks on the industry grew by 103%.
ATTACK RATE					
⚠ OVERALL	1.5%	1.2%	2.8%	4.8%	1.1%
DESKTOP	**2.0%**	**1.4%**	**3.9%**	2.6%	**1.3%**
MOBILE	1.4%	1.2%	2.3%	**6.1%**	1.0%

LexisNexis® RISK SOLUTIONS

Attack volume and attack rate 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

Slight Growth in Attack Rates Linked to Mobile Channels

Years of investment in technologies to protect consumers and consumer accounts, and rising consumer expectations for protection, have inadvertently made the consumer a prime vector for attackers. Around the globe, financial institutions have borne a surge of attacks via scams, unknowingly facilitated by legitimate customers deceived or manipulated to act against their best interests.

In growth markets, adversaries harvest consumer personal information via social engineering schemes (aka phishing), then attempt to profit from the consumer's identity. In mature markets, financial firms that have honed identity-based defensive measures struggle to detect when legitimate customers authorize fraudulent payments.

Financial services transactions in the Digital Identity Network grew by 17% in 2023, driven primarily by growth in EMEA and APAC. The human-initiated attack rate for financial services moved slightly higher to 1.2% (up 8% YOY). North America saw a significant increase in the attack rate (up 30%), which is all the more noteworthy considering that rates in APAC and EMEA fell 15% and 24%, respectively. Risk at the moment of payment (up 9% YOY) as well as at new account creation (up 12% YOY) has increased in 2023.

FINANCIAL SERVICES OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	The new account creation attack rate increased by 12% YOY, driven by increases on the mobile channel, primarily mobile browser.	Login attack rates remained stable in 2023.	The ultimate high-risk event for financial services organizations, payment attacks increased by 9% YOY, implying an increased financial risk for banks in 2023. Attack growth occurred most on the mobile channels.
ATTACK RATE			
OVERALL	8.3%	0.6%	5.6%
DESKTOP	10.3%	**0.8%**	4.5%
MOBILE BROWSER	**11.2%**	0.7%	**6.8%**
MOBILE APP	3.3%	0.5%	5.1%

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

Ecommerce: Overview of Trends and Attack Patterns

Customer Accounts Under Attack

Transactions from the global ecommerce industry rose modestly (7%) in 2023, as caution dictated behavior with interest rates and inflation rising around the world.

Where consumers held back, fraudsters dove in. Human-initiated attacks surged 80% YOY, resulting in an attack rate of 2.8% (up 59% YOY). A key component of this growth in attacks was a focus on account takeover of ecommerce accounts by the fraudsters, with the attack rate at login growing to 3.3% (up by 119% YOY). Attacks increased the most in North America and EMEA.

The significant rise in bot traffic volumes seen in 2022 persisted in 2023. Bots help bad actors to validate compromised identity or authentication data, either for exploitation via a human-initiated attack or for illicit resale on underground markets. They can also be used in more sophisticated password reset attacks.

ECOMMERCE OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Increased fraud on both desktop and mobile channels has driven the new account creation attack rate up to 7.3% (up 16% YOY).	The login attack rate has grown significantly again this year (up 119% YOY), with elevated risk on the mobile browser channel as existing customer accounts continue to be targeted.	The payment attack rate has grown moderately (11% YOY) with growth coming from the mobile channels.
ATTACK RATE			
OVERALL	7.3%	3.3%	2.4%
DESKTOP	**14.8%**	3.1%	**3.7%**
MOBILE BROWSER	4.0%	**5.7%**	2.8%
MOBILE APP	3.7%	1.3%	1.6%

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

LexisNexis® RISK SOLUTIONS

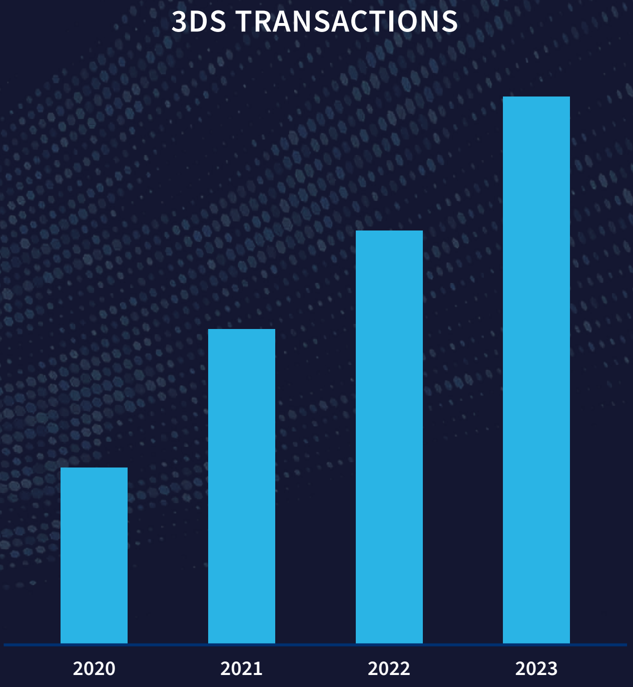
Powering 3D Secure with Digital Identity Intelligence

As more Card-Not-Present (CNP) transactions are routed via 3D Secure (e.g. due to existing PSD2 regulations in Europe; requirements in Japan from 2025 for all CNP traffic to go via 3DS) issuing banks seek not just additional assurances about consumers making purchases, but also more advanced risk signals. In particular, scams expose Access Control Server (ACS) providers that depend solely on authentication to reduce risk and have not updated their services to include robust and relevant digital intelligence.

A more comprehensive risk assessment strategy considers both unauthorized payments (e.g., stolen cards or compromised card data) as well as scam-related authorized payment fraud.

Issuing banks can access sophisticated scam signals through their 3DS channel, including:

- **Active call detection –** to understand better if a scam target is being coached into making a transfer
- **Social media app detection –** to identify elevated risk of specific scenarios, such as Facebook Marketplace scams
- **Historical and contextual user behavior –** to reveal complex cross-channel scam attacks



The Digital Identity Network assessed the risk of more than 1.9 Billion 3DS transactions in 2023. LexisNexis Risk Solutions partners with multiple ACS providers around the world.

Communications, Mobile and Media: Overview of Trends and Attack Patterns

After Several Years of Decline, Attack Rates Grow, Fueled by Accelerating Payment Fraud

The human-initiated attack rate for communications, mobile and media (CMM) grew to 4.8% in 2023 (up by 11% YOY), again the highest attack rate across the industries included in the LexisNexis Risk Solutions Cybercrime Report. The mobile app channel in particular showed growth in attack rates – almost doubling for both payments and new account creation use-cases. Financial scams are often perpetrated via compromised or malicious mobile numbers.

Bot traffic continued to drop (down 46% YOY) after a significant decrease in 2022.

Transaction volumes as a whole for CMM showed no growth for 2023, reflecting a subdued market after the rapid growth in traffic seen several years ago.

COMMUNICATIONS, MOBILE AND MEDIA OVERVIEW	**NEW ACCOUNT CREATIONS**	**LOGINS**	**PAYMENTS**
RISK TRENDS	Risk at new account opening dropped by 9% YOY, suggesting that tighter controls may be starting to deter some fraudsters. The mobile app attack rate did increase by 86% YOY.	Account takeover attack rates remained fairly stable between 2022 and 2023.	The payment attack rate almost doubled (up 95% YOY) in 2023, driven by strong attack growth via both desktop and mobile app channels.
ATTACK RATE			
OVERALL	12.2%	1.0%	4.1%
DESKTOP	13.7%	1.1%	3.9%
MOBILE BROWSER	11.9%	0.6%	3.3%
MOBILE APP	**14.5%**	**4.8%**	**4.4%**

Attack volume and attack rate 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

Quiet Before the Storm? Declining Attack Rates as Digital Transaction Growth Accelerates

2023 saw strong growth in gaming and gambling volumes (up 66%) as digital gambling became more regulated and available around the world. At a regional level, transactions increased by 76% in EMEA, 68% in North America and 48% in LATAM, while APAC volumes held relatively constant. Look for this trend to increase in 2024 as Brazil opens up to online casinos and India considers regulating digital gaming services.

The human-initiated attack rate declined slightly (down 3%) as good customer growth outpaced fraudster attack growth.

Automated attacks rose 103% year on year (driven by growth in EMEA and North America) as fraudsters used bots to test new services and compromised identity data, harbingers of future attacks.

GAMING AND GAMBLING OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account opening attack rates declined but remain significant. The desktop attack rate dropped significantly in 2023 (down 52% YOY).	The account takeover attack rate dropped by 33% YOY as good customer volume growth far outpaced growth in fraud volumes.	The attack rate at payment declined by 29% YOY following a similar trend at login.
ATTACK RATE			
OVERALL	7.6%	0.2%	1.0%
DESKTOP	**8.7%**	**0.7%**	**1.3%**
MOBILE BROWSER	7.3%	0.2%	1.1%
MOBILE APP	7.6%	0.2%	0.4%

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

CONCLUSION

Conclusion

2023 was another year of rising concern around the world as digital fraud, in particular scams in various guises, continued to increase and impact the public. Victims don't simply suffer financial loss but also psychological harm; however, a wider community of customer services and operations staff who have direct contact with the victims are also impacted emotionally.

Our first digital banking consortium, founded in the UK in 2019 by two early adopters, now facilitates collaboration between 10 active member organizations, with 37,000 net new contributions added on a near real-time basis every month. In 2023 new digital consortiums have been initiated in the United Arab Emirates and Singapore, emulating others around the world, confirming a desire to collaborate more closely to fight fraud.

While regulation will drive change longer term, at the time of publication, most countries do not have clearly defined and enforced reimbursement rules for victims of scams.

Regulation aside, organizations are putting measures in place to prevent fraud, as they are keenly aware of reputational risk (not to mention operational costs), in addition to actual monetary fraud losses.

Organizations show a continued focus on optimizing their fraud detection solutions. More banks are deploying multiple, targeted fraud models. For example, in Europe our Tier-1 banks all have a traditional, unauthorized fraud model deployed, but in addition, 71% have a separate model targeting authorized fraud and 29% have a dedicated mule detection model in place.

There are signs of hope. While scam attacks continue to grow around the world, the scam losses in the UK[1] and Singapore[2] appear to have stabilized, based on reported numbers for full year 2023.

These two countries have arguably suffered some of the greatest targeted attacks in their respective regions and have therefore also implemented (and continue to implement) significant defenses to try to protect consumers from financial loss and psychological harm.

[1] www.ukfinance.org.uk/news-and-insight/blog/what-did-2023-uk-finance-fraud-report-tell-us

[2] www.police.gov.sg/Media-Room/Police-Life/2024/02/Three-Things-you-Should-Know-About-the-Annual-Scams-and-Cybercrime-Brief-2023

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 at taking over user accounts using previously 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 (account creations, account login and payments) from mobile devices and computers received and processed by LexisNexis® Digital Identity Network®.

Attack Percentages are based on transactions identified as high risk and classified as attacks, by use case. 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 that target a transaction 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 cookieless 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. LexisNexis® ThreatMetrix® directly detects IP spoofing via both active and passive browser and network packet fingerprinting techniques.

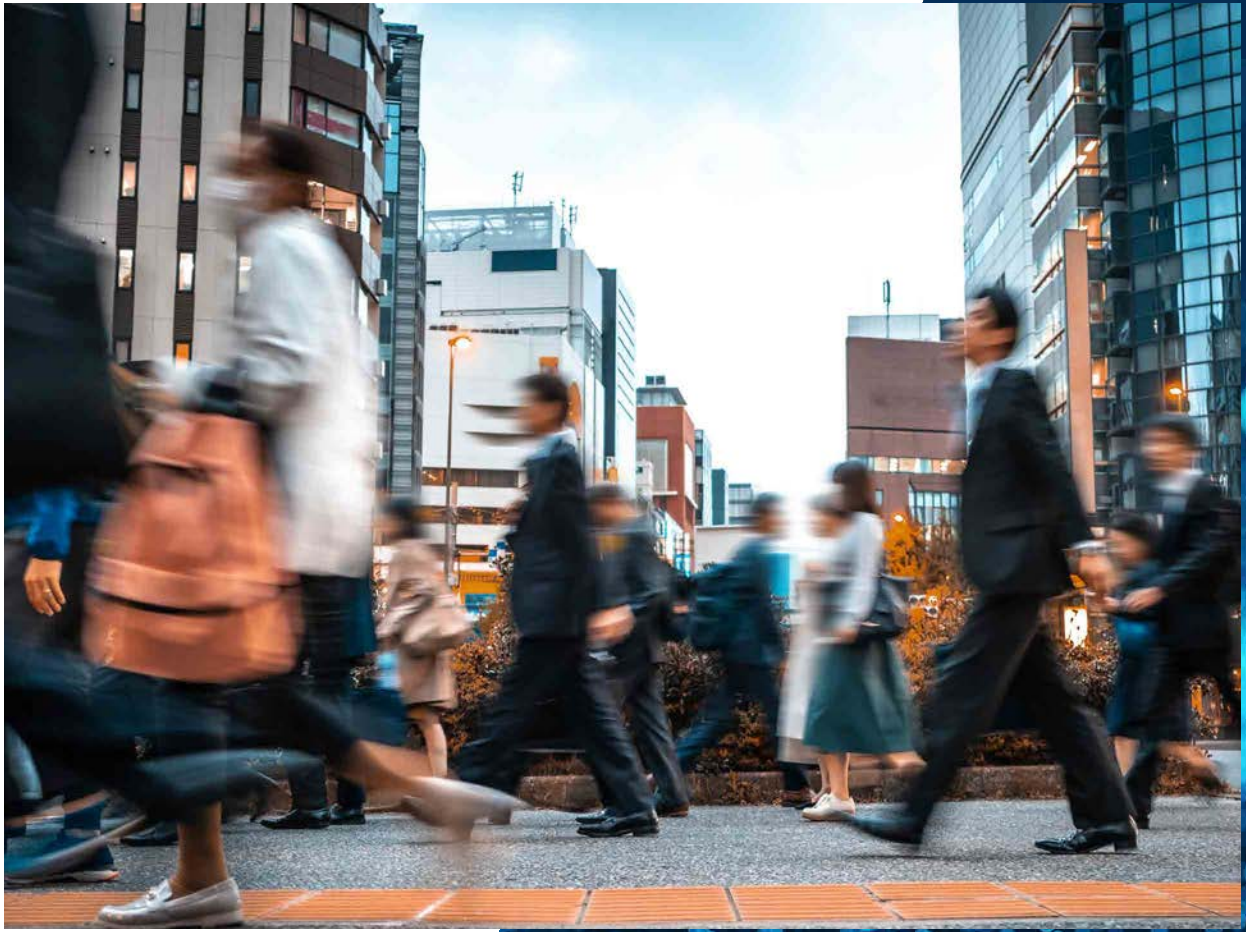
Man-in-the-Browser (MitB) and Bot Detection: Man-in-the-browser attacks use sophisticated trojans to steal login information and one-time-passwords from a user's browser. Bots are automated scripts that attempt to gain access to accounts with stolen credentials or create fake accounts and transactions.

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 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 the LexisNexis Digital Identity Network platform from January-December 2023, during near real-time analysis of consumer interactions across the online journey, including new account creations, logins, payments, password resets and monetary transfers.
- Transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioral analytics.
- The Digital Identity Network platform and its near real-time policy engine provide expansive and robust 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 for their unique 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.



LexisNexis® RISK SOLUTIONS

Data Processed and Analyzed

The LexisNexis Cybercrime Report analyzes a subset of 92 billion transactions, excluding non-transaction-based events such as feedback data and test transactions, as well as transactions from organizations that are considered outliers based on extremely high or zero recorded reject rates.

The Cybercrime Report uses these 92 billion transactions to calculate overall transaction volumes globally and by region (based on digital location intelligence). If location is not identified, then the input IP address supplied by the client is used. Where an organization does not send the input IP address (2.9B transactions in 2023), the session cannot be assigned to a region. These are mostly unknown sessions.

The subset of 92 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 speed fails to record complete profiling data.

Human-initiated attack volumes are calculated on a further subset of 84.2 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.

The Digital Identity Network platform processed over 109 billion transactions between January and December 2023.

LexisNexis® RISK SOLUTIONS

LexisNexis®
RISK SOLUTIONS

For More Information
risk.lexisnexis.com/fraudandidentity

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

LexisNexis® ThreatMetrix®
risk.lexisnexis.com/threatmetrix

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses 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 LexisNexis Risk Solutions and RELX.

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 Risk Solutions, 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 © 2024 LexisNexis Risk Solutions. NXR16418-00-0424-EN-US