LexisNexis®
RISK SOLUTIONS

Trust and Collaboration as **Foundations to Fight Fraud**

Keeping Good Customers Safe

The LexisNexis® Risk Solutions Cybercrime Report 2022

Introduction

JANUARY-DECEMBER 2022 ANALYSIS

TABLE OF CONTENTS:

A Heightened State of Alert

Digital fraud rose significantly in 2022 compared to 2021, with the global attack rate up 20% year-over-year (YOY)—continuing the early signs seen in 2021 as some economies re-opened. While parts of Europe were back in lock down for a brief period at the start of the year, most of the world was starting to look forward, beyond the pandemic, even if many Asian countries didn't re-open their borders to international travel until the middle of 2022. Cybercriminals had already been looking forward to expanding opportunities. Countries historically less impacted by fraud—Singapore for example—were being clearly targeted at the start of the year with a surge in fraud attacks. By the end of the year, not only was much of the world back open for business, but there was talk of a new global fraud pandemic. Scams of all kinds—both traditional account takeover through phishing attacks as well as sophisticated authorized push payment fraud—were frequently in the news. Reports of industrial-scale scam centers and gangs in Asia and Eastern Europe[1] confirm that scams have become the latest organized digital crime, operating professionally and cross-border.

As fraud levels and sophistication increase it becomes more important than ever to classify fraud into different types. Legacy fraud prevention approaches relying primarily on multi-factor authentication are insufficient as are basic, single-model fraud detection solutions or black box approaches. Multiple, machine learning optimized detection models are required, running in real time and targeting different methods of attack.

More than ever, understanding the customer journey and behavior can help identify potential attacks in their early stages and prompt a response—for example, a real time, in-app message to the end-user/customer confirming that they are about to make an unusual payment and to verify they are not being coerced into doing this can help bring about a last-minute sanity check and end an otherwise successful attack. Being able to tie together a 360-degree view of your customers across digital channels is also imperative to ensure fraudsters don't exploit weaknesses with a multi-channel attack.

The expanded digital economy is here to stay and continues to grow rapidly in emerging markets. Cybercriminals prey on new, inexperienced digital users, as well as on those organizations launching new services in the digital world—looking for vulnerabilities and opportunities. But the evidence shows that anyone can fall victim to a well-developed scam. We all need to step up our game and take the fight to the fraudsters.

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

- **Fraud classifications around the world**
- **How organizations are developing a better 360-degree view of their customers and the benefits of doing this**
- **Hunting mules with digital identities**

[1] *Selected sources: www.aljazeera.com/news/2022/4/13/in-thailand-chinese-gangs-recruit-the-desperate-into-phone-scams, www.asia.nikkei.com/Spotlight/The-Big-Story/Cyber-slavery-inside-Cambodia-s-online-scam-gangs, www.vice.com/en/article/n7zb5d/pig-butchering-scam-cambodia-trafficking, www.theguardian.com/world/2023/jan/29/everything-is-fake-how-global-gangs-are-using-uk-shell-companies-in-multi-million-pound-crypto-scams*

Global Risks

JANUARY-DECEMBER 2022 ANALYSIS

Global Highlights: January-December 2022

Transactions

+24% ▲	**Global transaction volume year-over-year (YOY)**
+29% ▲	Financial services transactions
+17% ▲	Ecommerce transactions
-22% ▼	Communications, mobile and media transactions
0%	Gaming and gambling transactions

Human-Initiated Attacks

+20% ▲	**Human-initiated attack rate YOY**
+31% ▲	Financial services attack rate
+29% ▲	Ecommerce attack rate
-27% ▼	Communications, mobile and media attack rate
-11% ▼	Gaming and gambling attack rate

Automated Bot Attacks

+27% ▲	**Automated bot attacks YOY**
+23% ▲	Financial services bot volume
+195% ▲	Ecommerce bot volume
-91% ▼	Communications, mobile and media bot volume
-33% ▼	Gaming and gambling bot volume

LexisNexis® RISK SOLUTIONS

Global Transaction Patterns in Numbers

Mobile App Transactions Dominate the Field of Play, as Customer Retention Becomes the Name of the Game

The growth in digital transactions continues to flourish despite a myriad of world events including armed conflict, inflation and an economic downturn. In 2022 the number of transactions analyzed in the Digital Identity Network® approached 80 billion.

A stable rate of new account creations confirms the change in focus of digital consumers away from the early pandemic days where new account growth had taken off around the world and especially across emerging markets.

The growth in logins dominates as consumers explore expanded digital service offerings. Organizations emphasize the need to provide a tailored journey for their customer base, knowing customer retention and upsell is where the value is rather than customer acquisition. Payments have also seen a healthy growth, despite recession alarm bells. Digital payment innovation and choice continue to draw consumers, with digital payment methods also being used to settle in store purchases as consumers return to physical shopping locations.

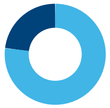
Mobile apps have become the preferred channel for digital transactions. Businesses, particularly in emerging markets, are several years into their digital transformation strategies and have prioritized mobile apps as a way to retain and upsell to their existing customer base. Originally the preserve of a select few super-apps, more and more organizations are expanding their in-app offerings, building an interconnected ecosystem within the app, ensuring their customers never need to leave.

TRANSACTIONS ANALYZED JANUARY-DECEMBER 2022

79.8B ········· Growth YOY **+24%** ▲

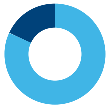
TRANSACTIONS BY CHANNEL

Desktop / **Mobile**



23% 77% ······· Growth YOY **+7%** ▲

Mobile Browser / **Mobile App**



18% 82% ······· Growth YOY **+8%** ▲

TRANSACTIONS BY USE CASE

		Growth YOY
New Account Creations	1.0B	+0.4% ▲
Logins	58.7B	+27% ▲
Payments	12.7B	+19% ▲

Global Attack Patterns in Numbers

Automated Bots for Harvesting, Human-Initiated Attacks to Reap the Rewards

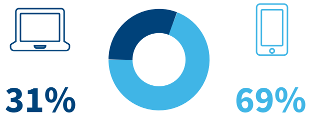
HUMAN-INITIATED ATTACKS

Attack rates on individual online transactions that typically return full digital identity data have seen a significant rise in 2022, outpacing the growth in good customer transactions, with attacks continuing to shift to the mobile channels.

ATTACK VOLUME

905M .... Growth YOY +56% ▲

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



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

+18% ▲

ATTACK RATE

		Growth YOY
Overall	1.3%	+20% ▲
Desktop	1.7%	+8% ▲
Mobile Browser	2.7%	+37% ▲
Mobile App	0.8%	+58% ▲

AUTOMATED BOT ATTACKS

Automated bot attacks (typically used to credential test stolen identities at high volume) have shifted focus away from the communications, mobile and media (CMM) industry in 2022, focusing now predominantly on the ecommerce sector.

ATTACK VOLUME

3.5B .... Growth YOY +27% ▲

		Growth/Decline YOY
Financial Services	1.9B	+23% ▲
Ecommerce	1.4B	+195% ▲
CMM	46M	-91% ▼
Gaming and Gambling	99M	-33% ▼

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.

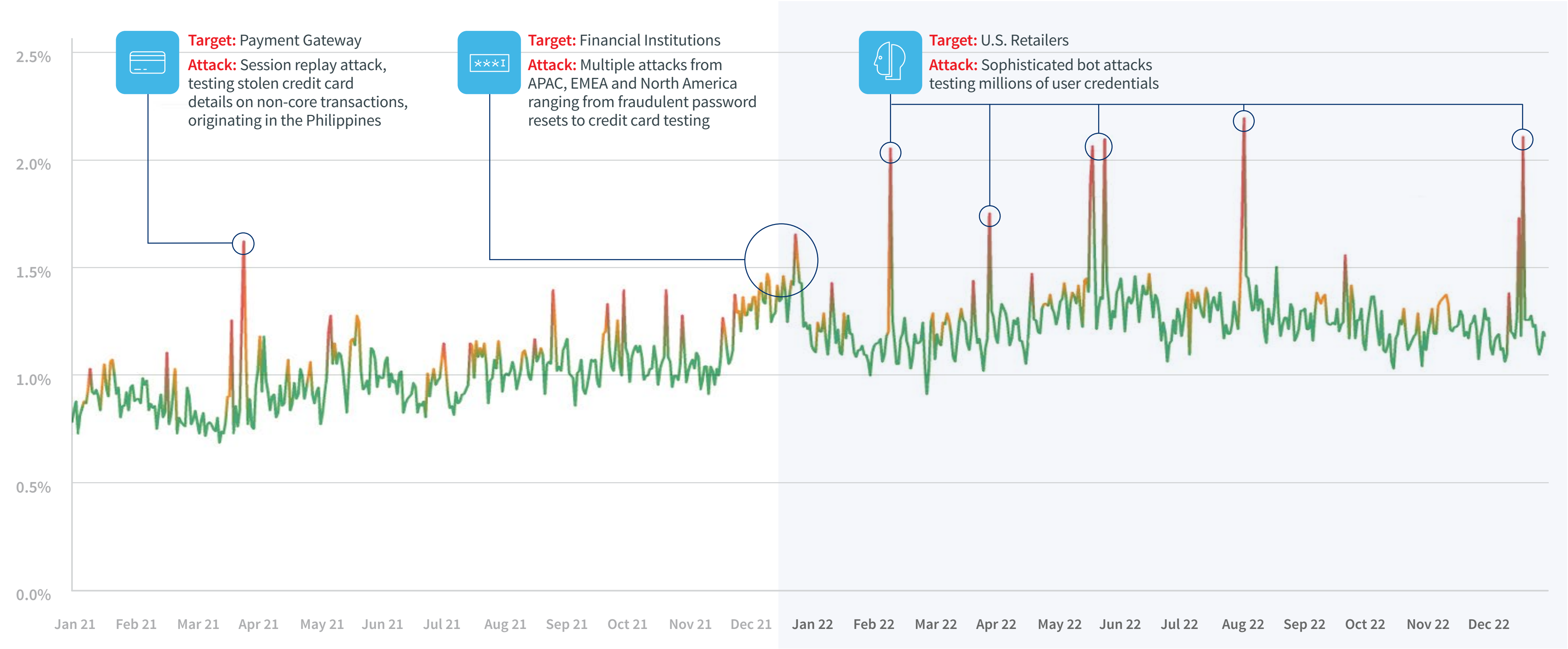
Identity Abuse Index

A Heightened State of Attack as the Pandemic Fades Away

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 rising trend seen during 2021 has been sustained in 2022, **with the identity abuse index rising 20% compared to 2021.**

IDENTITY ABUSE INDEX

● LOW ● MEDIUM ● HIGH



Target: Payment Gateway
Attack: Session replay attack, testing stolen credit card details on non-core transactions, originating in the Philippines

Target: Financial Institutions
Attack: Multiple attacks from APAC, EMEA and North America ranging from fraudulent password resets to credit card testing

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

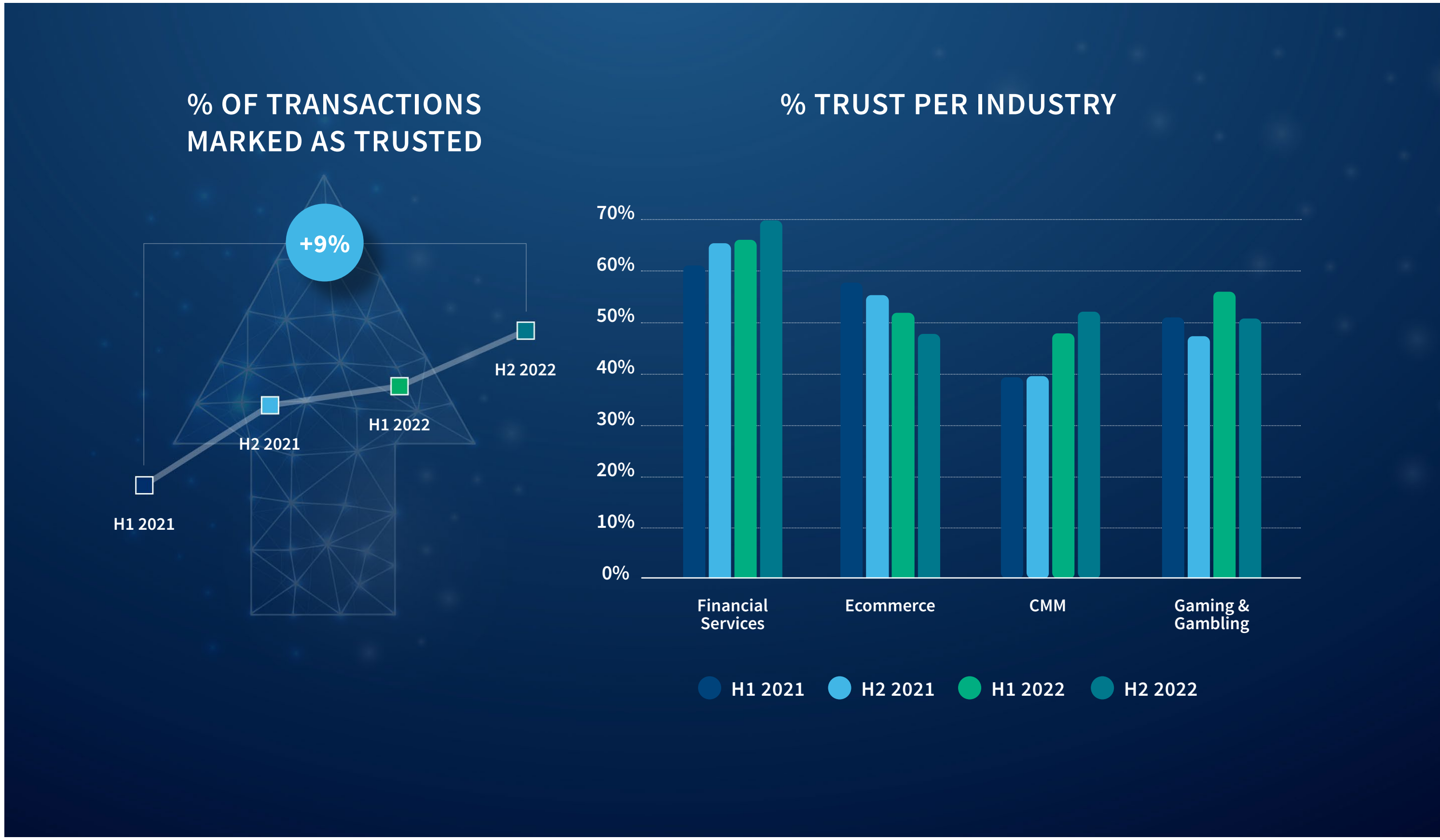
An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations from the medium-term trend.

The Need to Focus on Trust as Attack Rates Increase

How to Identify Your Good Customers

As fraud attacks increased during the last 18 months, organizations have responded by focusing more on building trust with their loyal customer base. Analysis from the Digital Identity Network® showed that the percentage of events classified as trusted during this period increased by 9%. Separating out the trusted population enables organizations to enhance the digital experience for good customers while facilitating a more focused analysis of the remaining events to determine which are attacks.

Seen at the industry level, trust has primarily been built in the communications, mobile and media (CMM) and financial sectors. Ecommerce shows a reversal of this trend, highlighting an inherent growing risk in this sector today, with high volumes of bot attacks and opportunities for fraud amongst the myriad of emerging payment methods available to consumers.

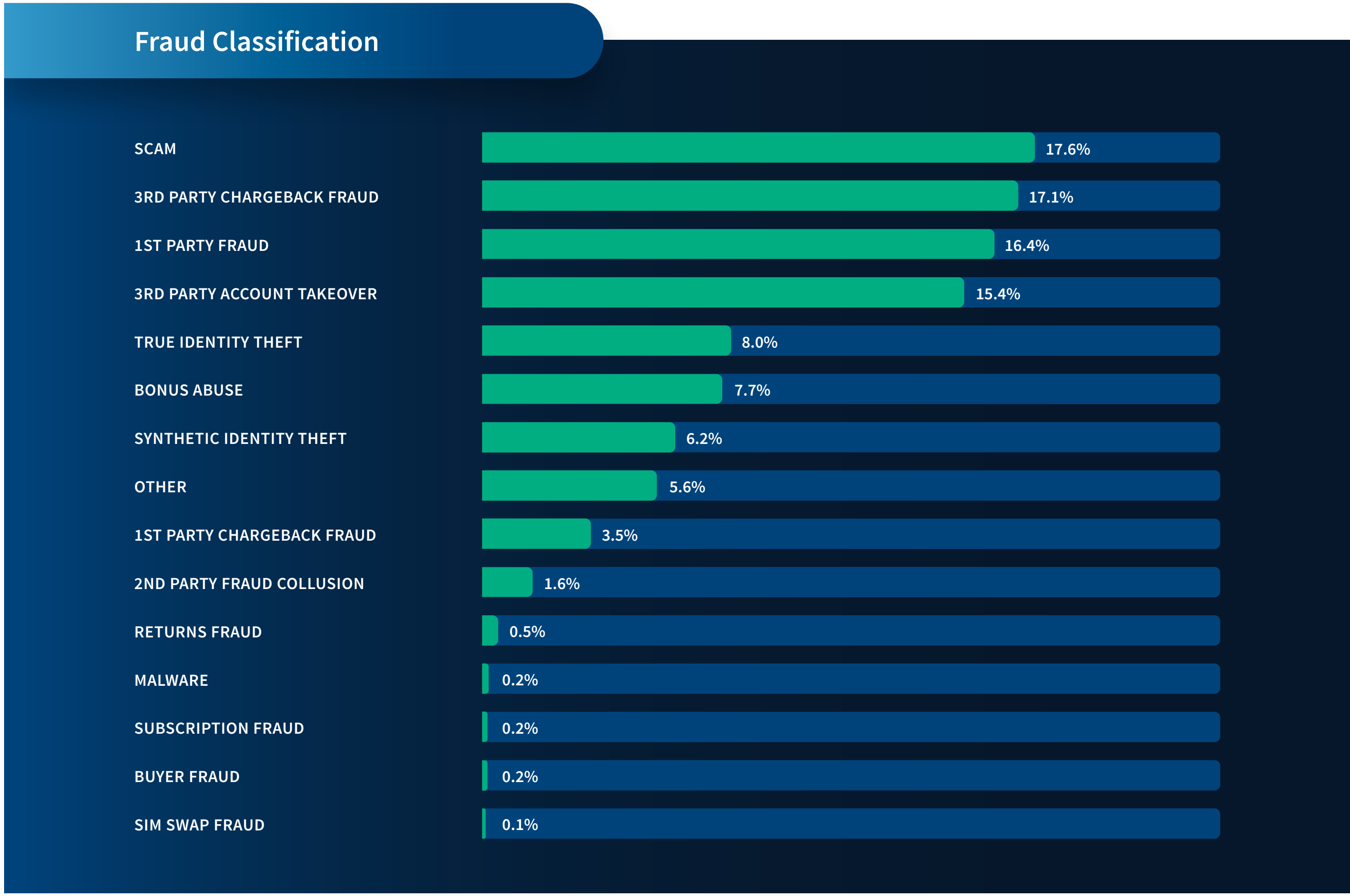


The Complexity of Digital Fraud

Fraud Classifications from a Client Perspective

As fraud becomes more complex, it is important to classify fraud attempts based on their context and modus operandi. Sophisticated fraud detection systems enable multiple, targeted models to assess risk in real time, looking for the anomalies associated with different types of attacks. Alerts generated by these models can be directed at different operational teams to be handled in different ways: for example, interaction with a potential victim would likely be different in a 3rd party account takeover scenario versus a suspected authenticated push payment scam.

The chart on this page shows how fraud attempts in the Digital Identity Network® are classified by our clients. Third-party account takeover, 3rd party chargeback fraud, scams and 1st party fraud are the four most common classifications in 2022, although the broad range of classifications highlights the breadth of use cases and industries using the network.



Fraud Classifications by Region and Industry

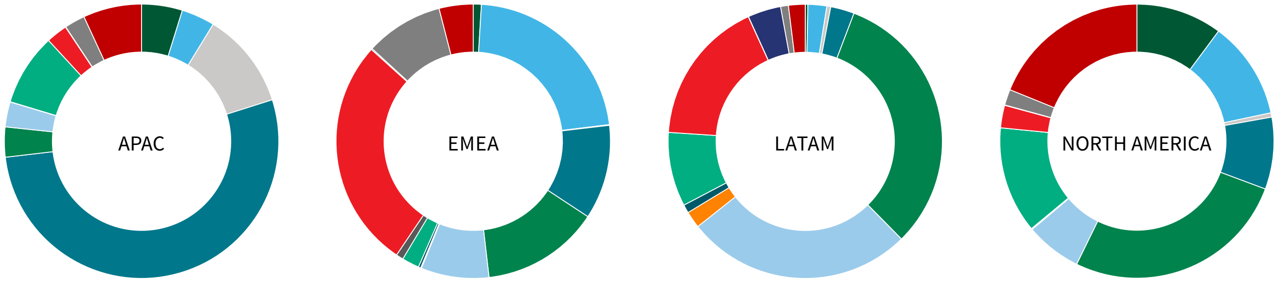
Geographical Differences Highlight the Need for Local Knowledge

Regional analysis of fraud classifications reveals significant differences. Third-party account takeover is the largest fraud classification for APAC, while scams predominate in EMEA. Third-party chargebacks are significant in LATAM and North America, with North America also showing a significant portion of true identity theft.

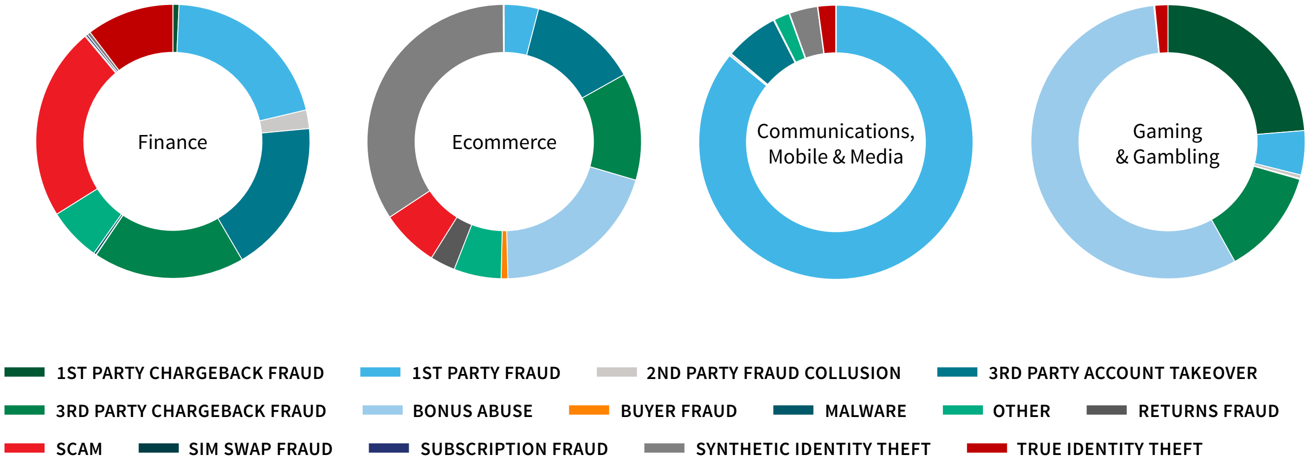
From an industry perspective, as expected, certain types of fraud are more prevalent than others for a particular industry: synthetic identity theft is predominant for ecommerce while the gaming and gambling industry suffers from significant bonus abuse at account sign-up. Scams are the largest issue for the financial sector.

Exact definitions and interpretations of various types of fraud (for example, scams) can vary across industry and region, making detailed comparisons challenging. Local nuances need to be understood to ensure fraud models are tuned correctly.

FRAUD CLASSIFICATION per region



FRAUD CLASSIFICATION per industry



A Consolidated Approach To Preventing Scams

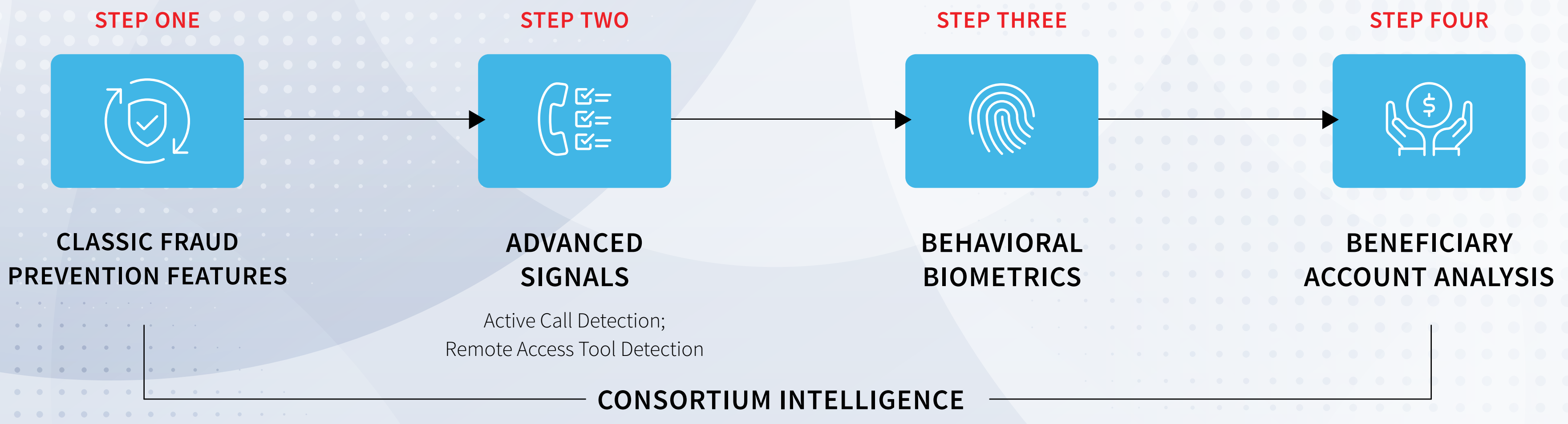
Bringing Together Data, Organizations and Technology

Social engineering scams are the largest threat facing financial institutions in terms of fraud. While phishing scams are still predominant in many parts of Asia, the more complex impersonation scams impacting the UK and some other countries—where the victim is convinced to move their own money into the fraudster's account (authorized push payment fraud)—will become more dominant in all parts of the world.

Many individual signals can provide clues to a scam being in progress: for example, classic fraud detection signals such as unusual amounts of money being transferred, or new advanced indicators around active cell phone calls being in progress during a payment attempt; behavioral biometric indications of hesitation or coaching of the victim; or risk associated with the destination account. Shared intelligence from across the industry can also identify attacks from specific cybercriminal gangs.

Advanced machine learning models with access to this range of information are able to identify many of these scams at the moment of payment. The challenge is often to ensure all signals across the user journey are available, in the same system as the fraud detection models, together with access to the consortium intelligence. Only then can these features work together in collaboration, with the correct weightage assigned to them, as so not to impact genuine customers.

Machine Learning Scam Model



LexisNexis® RISK SOLUTIONS

Hunting Mule Networks with Digital Identities

An Integral Part of the Scam Prevention Approach

Mules are often considered more of a financial crime problem, for example, they play a supporting role in money laundering or terrorism financing. However, mules also play a significant role in networked fraud schemes by providing accounts that can be used to receive stolen funds and a mechanism to rapidly transfer those funds onwards across banks and borders.

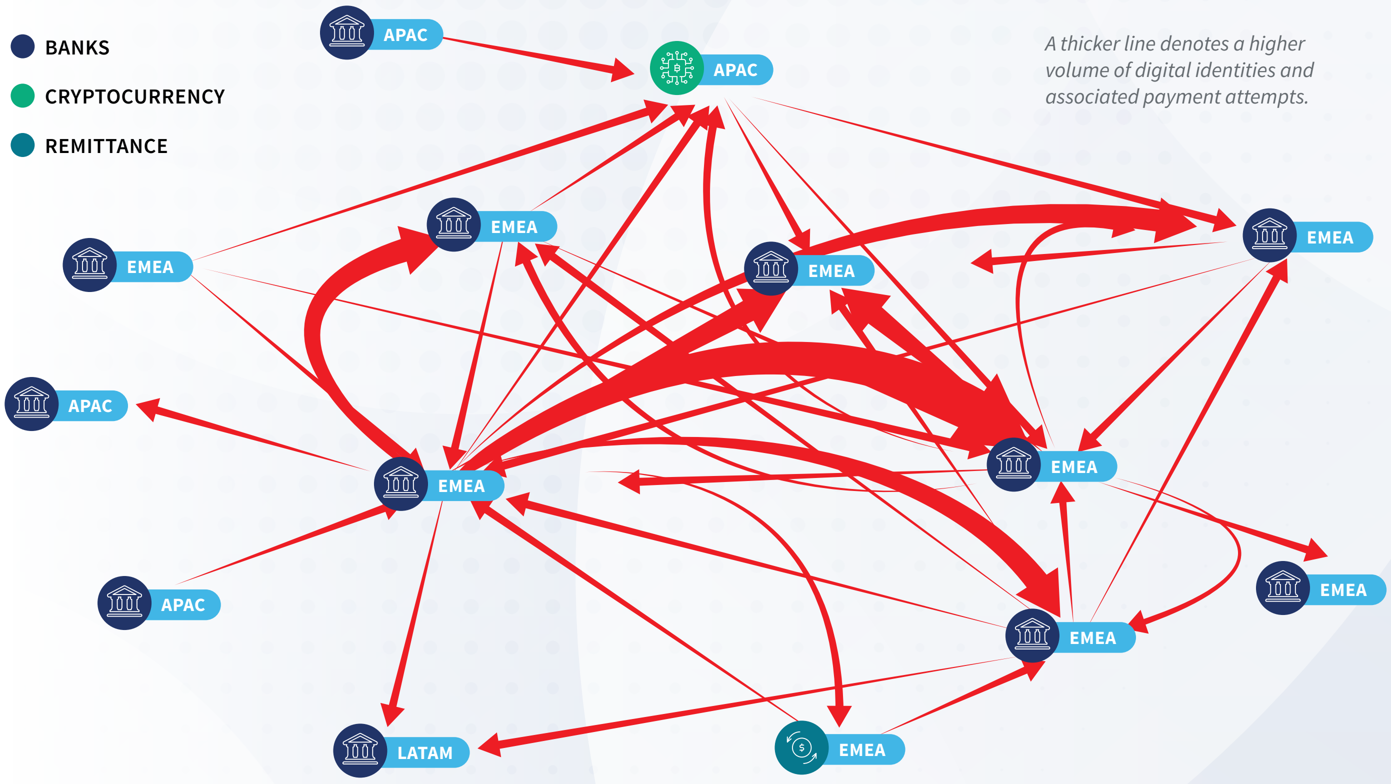
As the problem of digital fraud and scams increases, so does the reliance on mule accounts. There is no surprise that the growth in mule accounts has become a global issue.

Mules can also be classified into different types—complicit (accounts set up specifically for mule activity); converted (genuine accounts where the owner knowingly begins to engage in mule activity); unwitting (genuine accounts where owners are unwittingly scammed into mule activity)—requiring models targeted at different behaviors.

The Digital Identity Network® reveals mule operations at both a macro and micro level, together with the ability to analyze the data in multiple dimensions—for example, linked by payment flows or digital identity.

This visualization shows mule networks, linked by digital identity, operating during the last quarter of 2022 across financial institutions of different kinds and crossing multiple regions of the globe.

Each arrow illustrates digital identities associated with confirmed mule payment attempts at one organization, crossing over to another organization in the Digital Identity Network. Cross-over frequently occurs both ways.



A thicker line denotes a higher volume of digital identities and associated payment attempts.

Hunting Mule Networks with Digital Identities

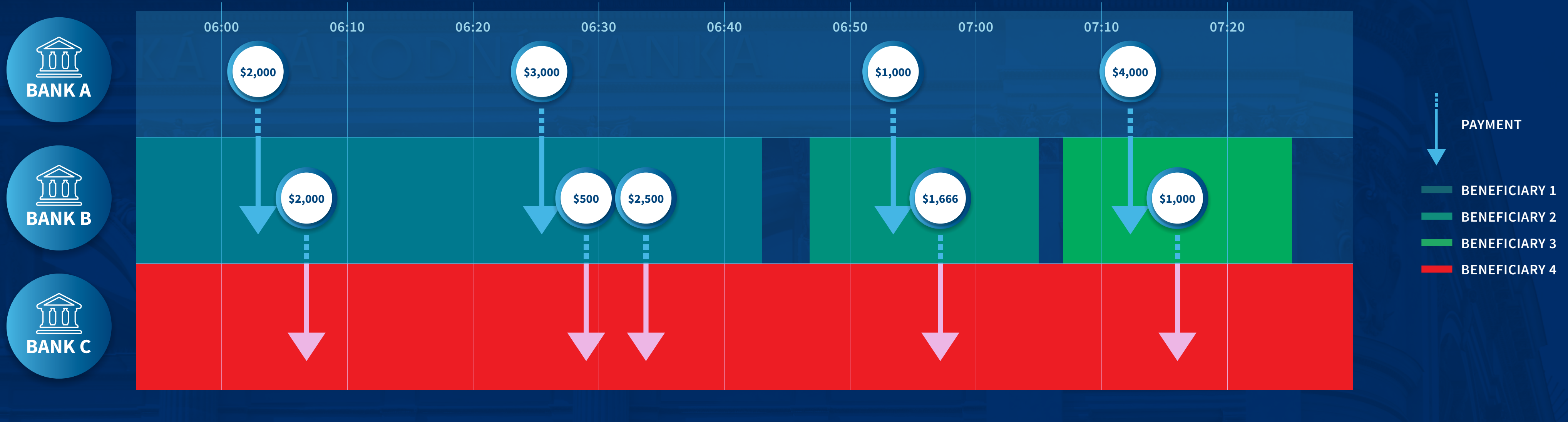
An Integral Part of the Scam Prevention Approach

The visualization shows a real example of money flows across accounts between different banks, linked by a single digital identity. Within a short period of time on a single day, multiple transfers are made.

Amounts are often very general values. Sometimes it is possible to see clear movement of the money between two accounts. Initial amounts may be broken down into smaller amounts before being moved on to the next account in the mule network. Some amounts are transfers to other banks that are not in the network.

As discussed in the previous LexisNexis® Risk Solutions Cybercrime report, an end-to-end scam prevention strategy must consider money flows into mule accounts. Without the ability to link by digital identity, these money transfers across banks in real time would be hard to disrupt and investigate.

Money Flows Through a Mule Network



Across the Customer Journey

JANUARY-DECEMBER 2022 ANALYSIS

Customer Journey Highlights: January-December 2022

New Account Creations

1 in every 11 new account creations are attacks

78% of new accounts are created via mobile channels, higher than all other use cases

Logins

104% YOY increase in attack rate through the mobile app channel

Highest volume growth across all use cases, **up 27%**

Payments

Highest growth in bot attacks across core use cases, **38% YOY**

Most frequently attacked use case by volume **on the mobile channel**

Password Resets

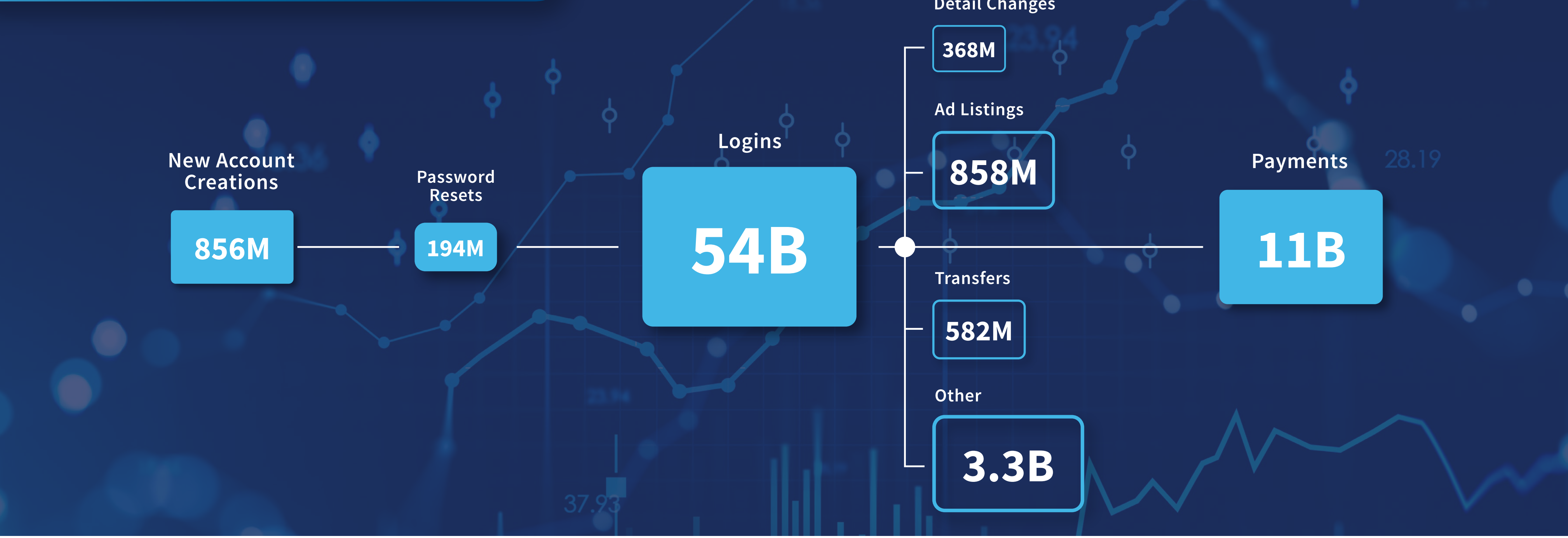
231% YOY attack rate growth via the mobile app channel

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



New Account Creations

856M

Password Resets

194M

Logins

54B

Detail Changes

368M

Ad Listings

858M

Transfers

582M

Other

3.3B

Payments

11B

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 Risk Increases Significantly with Payment Risk Also on the Rise

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Risk at new account creations remains stable for 2022, only slightly higher (3%) YOY, but consistently the highest risk in the customer lifecycle. New account creations occurring through the desktop channel are most likely to be fraudulent.	The shift in focus of cybercriminals to account takeover is revealed as login attack rates grow 52% YOY in 2022. Attack rates through the mobile app channel more than doubled (104%) YOY.	Payment attacks are the ultimate goal of most fraudsters. Attack rates on digital payments also saw significant growth in 2022, up 27% YOY, with broad increases across all desktop and mobile channels.
ATTACK RATE ⚠ OVERALL	9.2%	0.7%	3.7%
DESKTOP	**12.2%**	**1.1%**	4.1%
MOBILE BROWSER	10.2%	0.7%	**4.4%**
MOBILE APP	3.2%	0.5%	2.8%

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 Additional High-Risk Touchpoints

Password Reset Events Remain High Risk Despite a Drop in Attack Rates YOY

	PASSWORD RESETS	DETAIL CHANGES	AD LISTINGS	TRANSFERS	OTHER
RISK TRENDS	While attack rates have dropped 30% YOY, password reset events remain a high-risk customer touch point. Attack rates via the desktop channel have been declining (-46%) YOY, while the most growth comes from the mobile app channel up 231% YOY.	Fraudsters change email addresses and mobile numbers to ones they control to bypass security methods such as SMS one-time password. Attack rates via the desktop more than doubled in 2022 (up 109% YOY), while a strong decline was seen via the mobile app (-74%) YOY.	Ad listings allow fraudsters to control the sale or promotion of goods and services. This can provide a way of monetizing stolen goods, posting fake listings for properties or services, or creating phony reviews to facilitate sales. Overall attack rates for ad listings were stable, with an increase via the desktop channel offset by decreases on mobile channels.	Transfers enable money to be moved into a different account within a customer's overall profile. This action sometimes precedes a fraudulent payment event after an account takeover. Attack rates associated with transfers increased significantly in 2022 (up 64% YOY), driven by increase in the mobile channels.	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 were lower YOY (-23%), with only the mobile app channel showing growth.
ATTACK RATE					
OVERALL	5.8%	1.2%	0.6%	0.9%	1.0%
DESKTOP	**8.5%**	**1.8%**	**1.1%**	**1.6%**	**1.4%**
MOBILE BROWSER	1.6%	1.2%	0.8%	1.1%	1.2%
MOBILE APP	6.9%	0.4%	0.4%	0.7%	0.8%

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.

LexisNexis® RISK SOLUTIONS

A 360 Degree View of Your Digital Customer Base

Improved Risk Assessment Across the Customer Journey

While this section of the report focuses primarily on the risk associated with key touch points in the digital customer journey, a more complete assessment of risk can only occur when the full context of the customer's interactions with the mobile app or website is understood.

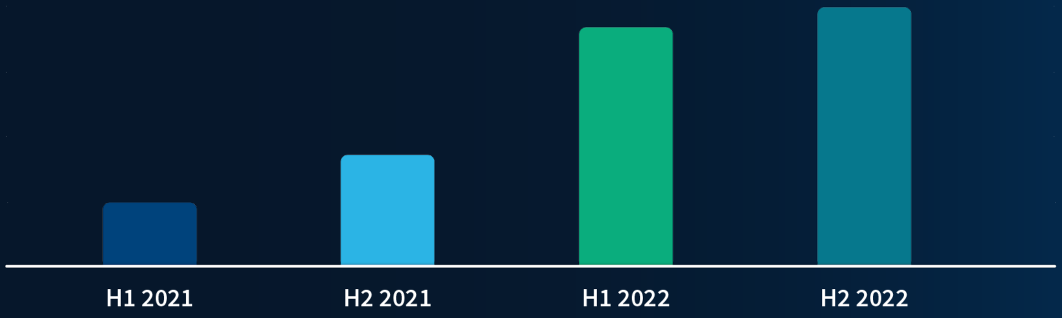
As fraud has become more complex, clients using the Digital Identity Network have moved away from single, point-in-time risk assessments to building up risk along the customer journey. The number of clients deploying the solution across all three core stages of a customer lifecycle (new account creations, logins and payments) is up 77% in 2022 compared to 2019. Gathering contextual digital intelligence at login can improve risk assessment at subsequent payment events by more than 60%.

Another important consideration is the different channels that customers can use to interact with digital services. At a simple level this can be ensuring that digital intelligence from browser and mobile app channels is consistent rather than siloed in different systems. From an industry point of view, this can mean ensuring that the same digital intelligence is used for risk assessments in ecommerce across digital channels as well as in physical stores where digital payment methods via the app are also offered.

In the financial sector, digital banking risk assessments are often clearly separated from Card-Not-Present (CNP) transaction risk assessment for issuing banks. There is technically no fundamental reason for this. **In 2022 the number of banks using the Digital Identity Network across both digital banking and 3D Secure CNP channels has grown significantly (133% YOY).**

On average, 82% of consumers who shop online with their credit card are also active online banking users from the same bank, meaning that digital identity intelligence can be shared across channels to drive trust and prevent more complex fraud.

BANKS LINKING DIGITAL IDENTITY INTELLIGENCE ACROSS DIGITAL BANKING AND 3D SECURE CNP CHANNELS



Regional Trends

JANUARY-DECEMBER 2022 ANALYSIS

Regional Highlights: January-December 2022

APAC

+31% ▲ transaction volume YOY

+38% ▲ human-initiated attacks YOY

-19% ▼ bot volume YOY

EMEA

+22% ▲ transaction volume YOY

+21% ▲ human-initiated attacks YOY

+75% ▲ bot volume YOY

LATAM

+93% ▲ transaction volume YOY

+102% ▲ human-initiated attacks YOY

-9% ▼ bot volume YOY

North America

+14% ▲ transaction volume YOY

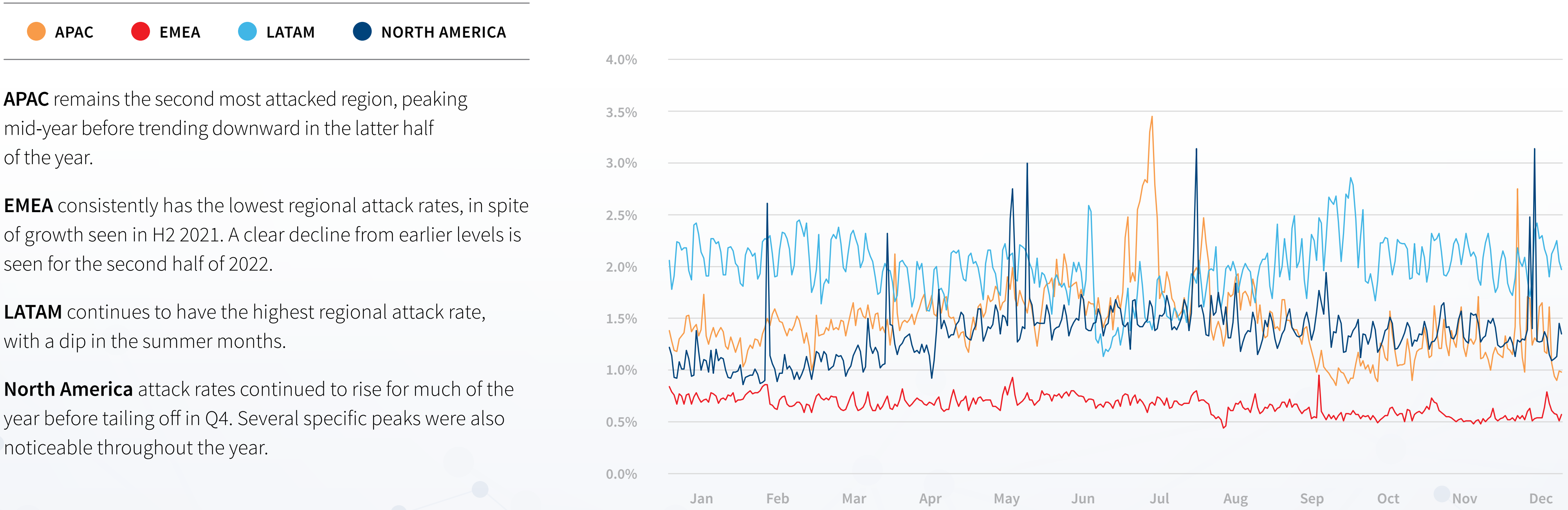
+57% ▲ human-initiated attacks YOY

+32% ▲ bot volume YOY

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

Identity Abuse Index by Region

Elevated Attack Rates Reducing in Q4 2022 in Some Regions



APAC remains the second most attacked region, peaking mid-year before trending downward in the latter half of the year.

EMEA consistently has the lowest regional attack rates, in spite of growth seen in H2 2021. A clear decline from earlier levels is seen for the second half of 2022.

LATAM continues to have the highest regional attack rate, with a dip in the summer months.

North America attack rates continued to rise for much of the year before tailing off in Q4. Several specific peaks were also noticeable throughout the year.

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.

Scams Proliferate in the Financial Sector as Automated Bots Target Ecommerce

Scams are central in everyone's mind in Asia Pacific at the end of 2022 as countries historically less targeted by fraud have been confronted with unprecedented levels of attack. It is important to note that in Asia specifically, the term "scam" is used as a general reference to all types of fraud where trickery of the victim is involved—not just coercion of a victim into executing instructions which may involve transferring money out of their own accounts, as is the case in the U.S., Europe or Australia. Reports in the regional press identify professionalized scam centers operating in various places and match with elevated fraud rates seen originating from those same areas.

Countries in the Asia Pacific region are in different stages of economic development and businesses are struggling to implement an effective fraud prevention approach that can address multiple regional challenges and fragmented market conditions across the region.

Payment fraud is seen as a huge opportunity for cybercriminals in APAC, as alternative payment methods continue their popularity in the region.

Payment transactions increased by 32% YOY, while the attack rate increased at 50% YOY. The proliferation of new payment methods, such as digital wallets, QR code payments, peer-to-peer transfers and to a lesser extent, Buy Now, Pay Later, require a more holistic approach that looks beyond basic device intelligence, but also combines digital intelligence, behavioral analysis and adaptive authentication.

APAC has a relatively unique ecosystem for ecommerce driven by super-apps, ecommerce led ecosystems which are inherently tied into other financial services via one interface. This gives the consumer the ability to use multiple monetary services via a "one stop shop". The consumer ease comes at a price, as fraudsters are increasing attacking the ecommerce industry in APAC with automated bot attacks (a 158% YOY increase), in an attempt to gain access to these apps through the take over of existing user accounts.

ATTACK SPOTLIGHT IN APAC JANUARY-DECEMBER 2022

- Concentrated fraud attacks on financial institutions in the region originating from Cambodia and Myanmar.
- High value transactional fraud attacks on regional digital banks routed via U.S. proxies.

APAC Transaction and Attack Patterns

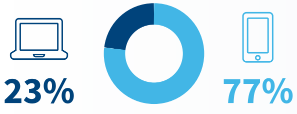
TRANSACTIONS

TRANSACTIONS ANALYZED

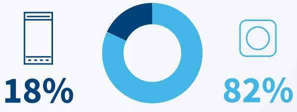
7.1B .... Growth YOY +31% ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

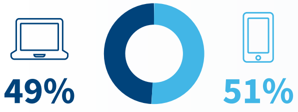
94M .... Growth YOY +38% ▲

AUTOMATED BOT ATTACK VOLUME

453M .... Decline YOY -19% ▼

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / Mobile



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

.... +15% ▲

LexisNexis® RISK SOLUTIONS

APAC Position Against Global Figures

APAC Mobile App Attack Rate is Half of the Global Average

APAC’s overall attack rate is higher than the global average. Mobile app transactions are significantly lower risk than desktop or browser transactions. The desktop attack rate in APAC is well above the global average.

Human-initiated attack rates have grown across the region for ecommerce and the gaming and gambling industry, as countries open up regulations.

	GLOBAL	APAC
OVERALL ATTACK RATE	1.3%	1.5%
DESKTOP ATTACK RATE	1.7%	3.1%
MOBILE BROWSER ATTACK RATE	2.7%	3.8%
MOBILE APP ATTACK RATE	0.8%	0.4%

Authorized Push Payment Scams Prove to be EMEA's Top Priority

Emerging Regulations to Focus on Liability

Geopolitical tensions, disrupted supply chains and low economic confidence all played a hand in the cost of living crisis hitting major parts of EMEA. These conditions are making consumers increasingly concerned and fraudsters increasingly opportunistic. Transactions in the region climbed up by 22% YOY, a trajectory far surpassed by increases in automated bot attacks which grew by 75% YOY. Bot attacks within the ecommerce industry grew by 473% YOY, as the shift to credential stuffing shifted from the communications, mobile and media market.

Scams are plaguing Europe's financial services industry by inflicting damages across customer experience, revenue margins and productivity. Authorized push payment scams have direct financial impacts for consumers and they also create indirect operational costs and productivity losses for the businesses working to resolve the disputes following a successful scam attack. Regulators are responding to rising scams with victim-focused regulations holding financial institutions liable for the financial damages of authorized push payment fraud and placing the onus on the bank to reimburse the victim. Regulatory guidance in some countries suggests a trend toward a 50/50 split of consumer fraud losses between the customer's bank and the beneficiary's bank.

Deepfakes and the expansion of Artificial Intelligence (AI) tools are opening new attack vectors for enterprising fraudsters—leaving financial services firms offering app-based services exposed to additional risks. Fraudsters are utilizing deepfakes and AI tools in conjunction with synthetic or stolen identities to bypass identity verification controls for creating and accessing accounts. This increases fraud risk at new account creation and other journey touchpoints. This challenge will continue proliferating as access to AI tools becomes more widely available to the general public.

Another ongoing consideration centers on protecting all channels and customer touchpoints with equal emphasis since attacks are split fairly evenly between mobile and desktop (57% to 43%). Today's customer journeys are dynamic and consumers in developed economies often transact across multiple devices: mobile, tablets, desktops and laptops. Consumers anticipate universally consistent, reliably secure and fast experiences over every channel and modality and are quick to abandon businesses that don't meet these expectations. At the same time, fraudsters look to exploit vulnerabilities across different channels in more complex attacks.

ATTACK SPOTLIGHT IN EMEA JANUARY-DECEMBER 2022

- Bonus Abuse attack on gambling site originating from Brazil, UK, Egypt, Kenya and Nigeria.
- Rise in social engineering to beat strong customer authentication checks on ecommerce transactions.

LexisNexis® RISK SOLUTIONS

EMEA Transaction and Attack Patterns

TRANSACTIONS

TRANSACTIONS ANALYZED

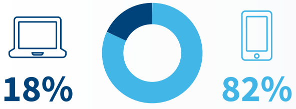
23.7B

Growth YOY

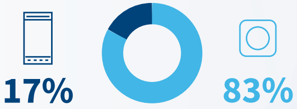
+22% ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

141M

Growth YOY

+21% ▲

AUTOMATED BOT ATTACK VOLUME

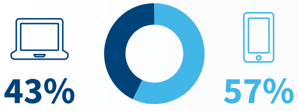
1B

Growth YOY

+75% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / Mobile



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

+7% ▲

EMEA Position Against Global Figures

Mobile App Transactions in EMEA are the Safest of all Regions

🌐 GLOBAL 📍 EMEA

EMEA has generally seen lower attack rates than the global average for several years due to the region's digital maturity and the high amount of trust built up between companies and digital identities.

Recent regulations enforcing the use of strong customer authentication as well as emerging regulations around scam liabilities continue to drive the focus on digital fraud prevention.

EMEA's attack rate on the mobile app channel is the lowest across any region.

	🌐	📍
OVERALL ATTACK RATE	1.3%	0.7%
DESKTOP ATTACK RATE	1.7%	1.6%
MOBILE BROWSER ATTACK RATE	2.7%	2.1%
MOBILE APP ATTACK RATE	0.8%	0.1%

Low Barrier to Digital Entry Gives Criminals Means to Clean Money

Neo-Banks and Fintechs are the Hub for Mule Accounts, as Crypto Exchanges are used to Launder

Latin American consumers are benefiting from an increase in digital companies and service in the region, which is lowering barriers for accessing financial services. The financial services sector in LATAM shows a 112% YOY increase in transactions. This market growth is also spurring sophisticated fraudsters and criminal networks to fully leverage easier consumer entry points to their complete advantage for the purposes of financial crimes and money laundering.

An example of this trend is seen in the popularity of PIX and other digital wallets in Brazil coinciding with the country experiencing a rise in QR code fraud. Similarly, Brazil had the 10th highest rate of crypto ownership/usage in the world during 2022[1] and the trend of using exchanges for nefarious activities is likely to keep increasing.

Automated attacks are causing ongoing challenges for LATAM's online retail sector where automated bot attacks on ecommerce businesses show a 26% YOY increase. Ecommerce companies are showing vulnerabilities at the payments touchpoint and fighting bot attacks utilizing card information from the dark web.

Brazil's economic activity increased by 2% in 2022 and ecommerce spending kept pace.[2] Ecommerce transactions in Brazil were up 54% YOY, however, nefarious bot attacks followed this trajectory in lockstep increasing by 66% YOY.

Social engineering scams, mainly carried out via vishing, smishing and phishing, top the LATAM region's biggest cybercrime challenges. LATAM's human-initiated attack volume increased by 102% YOY, underscoring the prevalence and problematic regional impacts of scams.

ATTACK SPOTLIGHT IN LATAM JANUARY-DECEMBER 2022

- Stolen/compromised credit card abuse originating from Brazil attempting to purchase cryptocurrency.
- Significant increase in scams at Mexican financial institutions.

[1] www.statista.com/statistics/1202468/global-cryptocurrency-ownership/
[2] www.worldbank.org/

LATAM Transaction and Attack Patterns

TRANSACTIONS

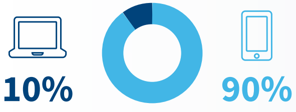
TRANSACTIONS ANALYZED

11.9B

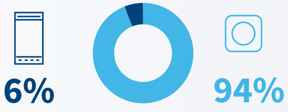
Growth YOY
+93% ▲

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

238M

Growth YOY
+102% ▲

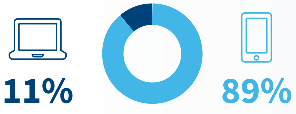
AUTOMATED BOT ATTACK VOLUME

279M

Decline YOY
-9% ▼

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / Mobile



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

+21% ▲

LATAM Position Against Global Figures

High Attack Rates Coupled with High Mobile Usage

🌐 **GLOBAL** 📍 **LATAM**

Attack rates in LATAM are consistently above the global average on all channels. This is primarily due to digital strategies in the region which are still evolving, coupled with a growing digital consumer base. The focus on acquiring new customers has resulted in a temporary imbalance toward prioritizing customer experience over fraud prevention. Digital fraud defenses are maturing.

The preferred channel of attack in the region is via the mobile browser. Over the last few years Latin Americans were a key part in the mobile revolution. This continues in 2022 where the mobile to desktop split is 90% towards mobile transaction—the highest across all regions.

OVERALL ATTACK RATE

🌐 1.3% 📍 2.0%

DESKTOP ATTACK RATE

🌐 1.7% 📍 2.2%

MOBILE BROWSER ATTACK RATE

🌐 2.7% 📍 4.1%

MOBILE APP ATTACK RATE

🌐 0.8% 📍 1.9%

LexisNexis® RISK SOLUTIONS

Automated Bot Volumes Problematic for North America

Gaming and Gambling and Ecommerce Facing Brunt of Bot Attacks

North America continues its relentless embrace of digital commerce and posts 14% YOY growth in transactions. Attack rates are also increasing with human-initiated attacks showing 57% YOY growth and automated bot attacks going up 32% YOY.

The region saw 1.7 billion bot attacks in 2022, underscoring North America's ongoing challenges with bots. Two industries are being highly targeted by bots: ecommerce showing a 127% YOY increase in the bot attack rate and the gaming and gambling sector posting 112% YOY growth in bot attacks. This significant rise in gaming attacks follows the region's forward progress in legalization driving increases in the number of licenses granted to sportsbooks. Bonus abuse is particularly rife in the U.S. gaming and gambling sector.

North America's ecommerce industry is contending against an increase in Card-Not-Present fraud facilitated by automated bot attacks. Increasing numbers of chargebacks are another significant challenge for the ecommerce sector with a notable rise in friendly fraud via chargebacks occurring in the holiday season. Friendly fraud typically involves consumers purchasing goods online while then claiming that the products do not work or have not been delivered.

The region's financial services industry is also facing a 42% YOY increase in human-initiated attacks. Many of these attacks are tied to impersonation scams where fraudsters posing as bank employees or government officials coerce victims into transferring funds into a fraudulent account.

ATTACK SPOTLIGHT IN NORTH AMERICA JANUARY-DECEMBER 2022

- Targeted bot attacks on ecommerce organizations from Vietnam, Pakistan, Germany, Spain, U.S. and Brazil.
- High-velocity credit card testing attack on non-profit organization originating from Iraq.

North America Transaction and Attack Patterns

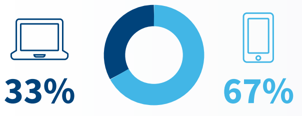
TRANSACTIONS

TRANSACTIONS ANALYZED

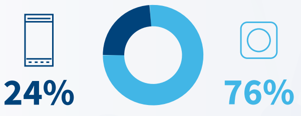
34.4B .... Growth YOY +14% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**



Mobile Browser / **Mobile App**



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

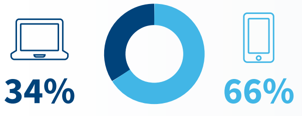
416M .... Growth YOY +57% ▲

AUTOMATED BOT ATTACK VOLUME

1.7B .... Growth YOY +32% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**



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

.... +14% ▲

LexisNexis® RISK SOLUTIONS

North America Position Against Global Figures

Mobile App Attack Rates Growing Rapidly

GLOBAL   NORTH AMERICA

North America's risk profile is slightly higher than the global average, with only the desktop attack rate below global levels.

The region sees the largest percentage of transactions still coming from traditional non-mobile channels—with desktop still accounting for 33% of all transactions.

The attack rate in the mobile app channel has grown 69% YOY, the highest in any channel.

	GLOBAL	NORTH AMERICA
OVERALL ATTACK RATE	1.3%	1.4%
DESKTOP ATTACK RATE	1.7%	1.4%
MOBILE BROWSER ATTACK RATE	2.7%	2.8%
MOBILE APP ATTACK RATE	0.8%	0.9%

Industry Opportunities

JANUARY-DECEMBER 2022 ANALYSIS

Industry Overview:
Overview of Trends and Attack Patterns

Ecommerce and Financial Institutions Suffer Elevated Attack Rates

INDUSTRY OVERVIEW	ALL INDUSTRY SUMMARY	FINANCIAL SERVICES	ECOMMERCE	COMMUNICATIONS, MOBILE AND MEDIA	GAMING AND GAMBLING
RISK TRENDS	The increase in attack rate in 2022 has come from financial services and the ecommerce industries.	The attack rate in financial services has increased by 31%, entirely driven by the mobile channel.	Desktop and mobile attack rates have both grown by 30%+ YOY, supported by high levels of automated bot attacks.	While the CMM industry maintains the highest overall attack rate, the rate decreased 27% YOY.	The gaming and gambling industry has seen a 51% YOY increase in desktop attack rate.
ATTACK RATE ⚠ OVERALL	1.3%	1.1%	1.7%	4.3%	1.1%
DESKTOP	**1.7%**	**1.3%**	**2.7%**	2.3%	**1.8%**
MOBILE	1.1%	1.1%	1.3%	**5.7%**	1.0%

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

Mobile Continues to Drive Increased Attack Rates

A few factors shaped the financial industry in 2022; the rising interest rate—which affected loan demand, deposit growth and profitability, along with digital banks focusing on revenue realization and diversification—for example, acquiring companies with lending products.

As fraud attacks on the sector rise globally, banks may also be more exposed to liability costs for scams in the near future. Organizations are exploring additional fraud detection capabilities like behavioral biometrics and active call detection.

Banks are also finding ways, such as embedded finance or banking-as-a-service, to provide services via non-conventional methods to increase customer retention and drive a wider revenue stream—potentially widening exposure to cybercrime activity.

FINANCIAL SERVICES OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account application attacks increased moderately YOY (12%) driven by attacks on the mobile channel.	As banks offer more services via their banking app, genuine transactions are rising, but attacks have the edge in 2022, with the attack rate for logins increasing by 69% YOY, driven by the mobile channel.	The payment attack rate increased 36% YOY, supported by a 56% YOY increase in automated bot attacks attacking the payment channel in financial services.
ATTACK RATE ⚠ OVERALL	7.5%	0.6%	5.1%
DESKTOP	**10.7%**	**0.8%**	4.4%
MOBILE BROWSER	9.7%	0.7%	**6.1%**
MOBILE APP	3.2%	0.5%	4.5%

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.

Country Level Networked Fraud Attacking Financial Institutions

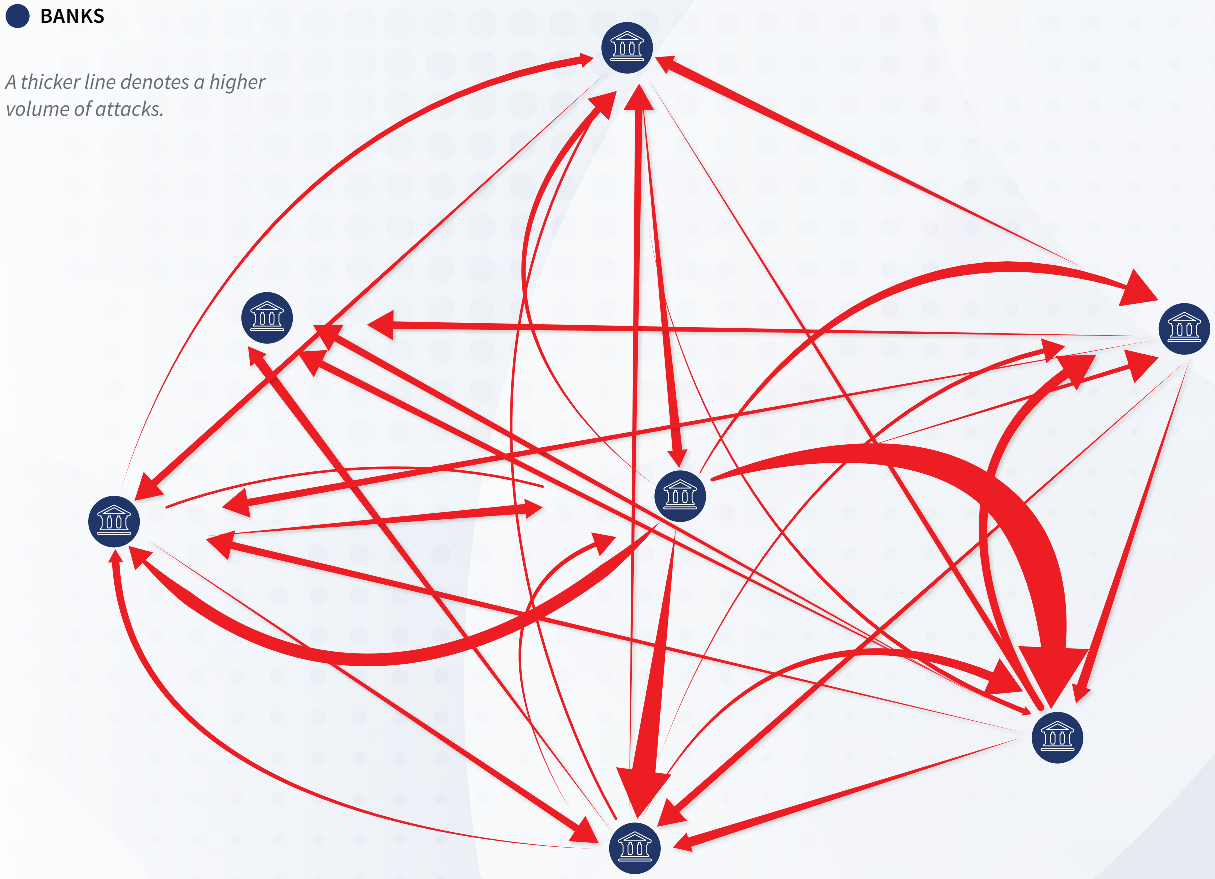
Singapore Example Representative of Any Financial Hub

This visualization shows a country-level fraud network (linked by digital identity) targeting financial organizations operating in Singapore during the second half of 2022. As fraud rates have risen globally in the last 12-18 months across financial institutions, similar networks can be identified for many individual countries.

Each dark blue circle represents an individual organization, while the arrows show fraudulent digital identities targeting the next bank having already launched an attack at the first organization. Line thickness reveals which directional flows are more common for cybercriminals.

The visualization reveals just how interconnected the fraud attacks can be at the country level—as well as the potential power of being able to share digital intelligence in real time to defend against these attacks.

Each arrow illustrates digital identities associated with confirmed fraud attempts at one organization, crossing over to another organization in the Digital Identity Network.



A thicker line denotes a higher volume of attacks.

Ecommerce: Overview of Trends and Attack Patterns

Bots Target Ecommerce Across the Customer Journey

The Digital Identity Network® saw a 17% YOY rise in transactions from the global ecommerce industry in 2022, as companies leverage data to heavily personalize the shopping experience for online customers.

Bot attacks in the industry seemed to be the biggest issue as the industry saw 195% YOY increase in overall bot attacks, with bots not only targeting the conventional customer touchpoints of new account creation (233% YOY growth), logins (153% YOY growth) but also change of details events, which had the highest growth in bot attacks at 441% YOY. This emphasizes the need for ecommerce players to protect the entire digital customer journey, as once the fraudster has the opportunity to change details, they could change the shipping address or phone number to illegitimately receive one-time passwords (OTP).

Buy Now, Pay Later (BNPL) payments continue to be attractive, especially with the younger generations. As rising interest rates make borrowing more expensive, the BNPL payment method for ecommerce will continue to be popular.

ECOMMERCE OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account creations saw a rise of 39% YOY of attacks via the mobile app channels, as more consumers (and fraudsters) move to enriched mobile app experiences. However, desktop attack continues to be the preferred target touchpoint with almost 1 in every 8 transactions being attacked.	Attacks on the desktop channel have grown 71% YOY and continue to be the leading attack channel, however, the most growth is seen in the mobile app channel with attack rates rising at 107% YOY.	The ecommerce payment fraud attack rate sees steady growth (11% YOY). The largest growth coming from mobile browser (up 40% YOY), while mobile app attack rates remain unchanged YOY.
ATTACK RATE			
⚠ OVERALL	6.3%	1.5%	2.2%
DESKTOP	**11.8%**	**2.2%**	**3.8%**
MOBILE BROWSER	4.0%	0.8%	2.1%
MOBILE APP	2.1%	1.0%	1.4%

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.

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

Attack Rates Decline for Logins and Payments

While the communications, mobile and media (CMM) industries continue to have the highest attack rates across industries in 2022, there is a noticeable decline seen in both the human-initiated attack rate and bot attacks. This suggests a subtle change in focus by cybercriminals.

During the pandemic mobile communications were more important than ever and there was a strong appetite for streaming services. Fraudsters took advantage of this in multiple ways, creating new fraudulent accounts and taking over existing ones. Streaming services were resold, and wireless contracts were used in complex attacks on financial services.

Organizations have responded by tightening up controls to try to combat scams initiated via mobile channels. Streaming providers are restricting shared accounts and targeting account abuse. Attacks on this sector are not going away, but cybercriminals are exploring what other, easier targets are available.

COMMUNICATIONS, MOBILE AND MEDIA OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	The high attack rate for new account creation (highest across all industries) remains constant YOY as fraudsters continue their focus on creating new CMM accounts.	The highest attack rate is on the mobile app channel, although this rate has declined 56% YOY.	The payment attack rate for CMM has declined by 27% YOY, with reductions across all channels except mobile app, which remained steady.
ATTACK RATE			
⚠ OVERALL	13.3%	1.0%	2.1%
DESKTOP	**15.5%**	0.7%	2.4%
MOBILE BROWSER	13.0%	0.9%	**2.8%**
MOBILE APP	7.8%	**4.4%**	1.9%

Gaming and Gambling:
Overview of Trends and Attack Patterns

Stable Attack Rates While Cybercriminals Assess Expanding Opportunities

The industry saw a promising 2022 with the regulators in two mass markets (U.S. and India) legalizing online gambling in more and more states. Online gambling became more commonplace during the pandemic and an economic downturn tends not to impact levels of gambling significantly. Transaction volumes seen in the Digital Identity Network remained constant year-over-year (YOY).

While attack rates as a whole declined slightly (-11% YOY), the desktop attack rate for new account creation is the highest rate (18.1% YOY) compared to all other industries. Bonus/promotional abuse is the primary issue for the industry, where fraudsters attempt to exploit offers multiple times.

A growing trend within the industry is to accept crypto payments due to their ability to process transactions almost instantly, allowing punters to make deposits and withdrawals easily—but also providing an attractive option for fraudsters.

GAMING AND GAMBLING OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Although attacks on new account creations have increased by only 5%, the desktop channel has the highest risk profile compared to all industries, with almost 1 in every 5 being an attack. Attacks on mobile apps have also increased by over 100% YOY.	Login attacks decreased from the year before (down 49% YOY), driving a decrease in the overall attack rate for gaming and gambling.	Payments transactions grew by 15% YOY, while the attack rate on the payment channel declined slightly (-5% YOY).
ATTACK RATE			
OVERALL	8.8%	0.4%	1.4%
DESKTOP	**18.1%**	**0.9%**	**1.9%**
MOBILE BROWSER	7.1%	0.3%	1.6%
MOBILE APP	7.2%	0.2%	0.5%

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 Fraud Network

This visualization shows regional fraud networks (linked by digital identity) targeting gaming and gambling operators during the last quarter of 2022. Each dark blue circle represents an individual organization.

It is likely that the network comprises several groups of cybercriminals, loosely connected across regions, using shared lists of stolen or synthetic identity data.

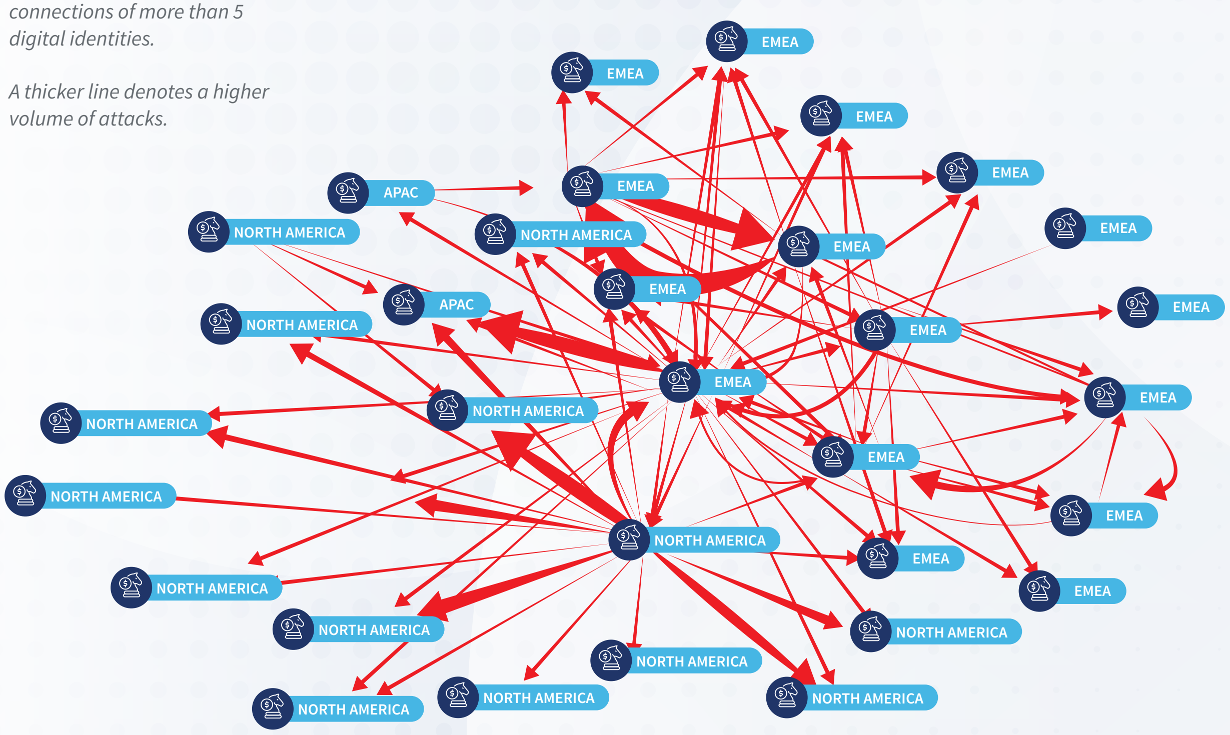
This network considers multiple event types—including new account creations, logins and payments, potentially revealing not just bonus abuse fraud but also payment fraud and money laundering activity.

Each arrow illustrates digital identities associated with confirmed fraud attempts at one organization, crossing over to another organization in the Digital Identity Network.

● GAMING AND GAMBLING ORGANIZATION

This fraud network only shows connections of more than 5 digital identities.

A thicker line denotes a higher volume of attacks.



LexisNexis® RISK SOLUTIONS

Conclusion

Conclusion

2023 was welcomed in with fireworks and celebrations reminiscent of turn-of-the-century euphoria as the pandemic truly faded from the public stage, with revitalized lunar new year celebrations following shortly after. The festivities also disguised a hint of anxiety spreading around many parts of the world as the economic outlook took a turn for the worse, fueled by rising interest rates, volatile energy prices and universal economic growth concerns. The expanded global digital economy is here to stay, but will 2023 see a downturn in transactions?

One thing is certain: cybercriminals won't be taking a break. Crime in general tends to increase during periods of economic crisis and opportunity in the digital world is rife. Vulnerable or hard-up citizens who have no intention of committing crime may still be lured into playing a complicit role in the world of mules.

Many digital services remain inadequately protected against sophisticated scam attacks, relying on multi-factor authentication as a single line of defense, without further layers of fraud detection built upon the analysis of digital intelligence and the anomalous behavior it can reveal.

The elevated attack rates seen around the world in 2022 are unlikely to decline in 2023, although investment in public education around the risks of scams, closer regulatory scrutiny and technical innovation may result in those attack levels plateauing. The challenge for organizations, industries and countries is to tie their digital intelligence together: to identify the interconnected signals of a complex fraud attack as it occurs, understand the behavioral anomalies it reveals and track down the subsequent money flows.

The good news is that there are already pockets of success—machine learning optimized scam detection models showing high detection rates; organizations working together to share intelligence in real time to prevent replicated attacks from organized fraud rings; the arrest of mule herders and closure of mule accounts. It is time to accelerate these initiatives and proactively take the fight to the cybercriminals.

Glossary, Methodology and Contact Details

Glossary

Industry Types

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

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

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

Gaming and Gambling includes online gambling and egaming services.

Common Attacks

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

Account Login Fraud: Attacks targeted 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 the 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.

LexisNexis® RISK SOLUTIONS

Summary Methodology

Overall Report

- The LexisNexis Risk Solutions Cybercrime Report is based on cybercrime attacks detected by the LexisNexis Digital Identity Network (the Digital Identity Network) from January-December 2022, during near real time analysis of consumer interactions across the online journey, from new account creations, 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.
- The 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.

LexisNexis® RISK SOLUTIONS

Data Processed and Analyzed

The overall volume of transactions processed by the Digital Identity Network January-December 2022 was 92 billion.

The LexisNexis Cybercrime Report analyzes a subset of these transactions that excludes 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. This subset totals 79.8 billion transactions.

The Cybercrime Report uses these 79.8 billion transactions to calculate overall transaction volumes globally and by region. There are 2.8 billion 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 79.8 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 71.2 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.

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 harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. 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.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis® 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.

For more information, please visit risk.lexisnexis.com and relx.com