LexisNexis®
RISK SOLUTIONS

Balancing Risk & Reward

The New Mobile Battlefield

The LexisNexis® Risk Solutions Cybercrime Report | July to December 2021

Introduction

JULY-DECEMBER 2021 ANALYSIS

Fraud Returns As Economies Reopen

Although the final weeks of 2021 will be remembered for the resurgence of the pandemic, driven by the new Omicron strain, the second half of the year actually marked the end of restrictions and the reopening of economies in many parts of the world. Especially in Europe, the Middle East and Africa (EMEA) and North America, consumers returned to physical stores and offices and travel began to resume, although the trend to digital services enforced by the pandemic showed no signs of reversing. What has also become clearly apparent from analysis of the LexisNexis® Digital Identity Network®, is that fraud is on the rise as consumer confidence returns. As consumers globally continue to drive demand for a customer-centric digital world, companies are prioritizing their digital customer excellence strategies to retain and acquire new customers, which is advantageous for legitimate consumers, but may lead to opportunities for fraudsters.

Consumers from mature digital markets continue to transact online, but emerging markets are truly leading the way in embracing the digital journey and driving growth in the network – often bypassing traditional browser interactions altogether and going straight to mobile apps. For the first time, the mobile share of transactions in the network reached 75% as app-based companies and industries increase in dominance. The underbanked are choosing easily accessible digital banking solutions, retail investors are embracing cryptocurrency exchanges and Buy Now Pay Later (BNPL) is seeing global popularity in the payment landscape.

While fraudsters are continuing their use of automated bot attacks seen throughout the pandemic, the human-initiated attack rate seen in the network rose for the first time since 2019, with financial services being the clear target. As anticipated for some time, fraudsters are now starting to capitalize on the fruits of their bot labors during the pandemic, using them in sophisticated attacks and scams. While fraudulent account creations remain a high risk, account takeover attempts have been increasing rapidly. No regions of the world appear immune to these attacks as governments, celebrities and the financial industry fight back with scam education campaigns. The ability to clearly recognize known, trusted customers at the moment of account access while identifying anomalies associated with any requests to reset passwords or change account contact details, is crucial in the fight against these relentless criminals.

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

- **Increased consumer dependence on the mobile channel and how fraud patterns have changed accordingly**
- **The sophisticated fraud networks linking finance and telecommunications**
- **The level of detail and complexity of frauds carried out by individual fraudsters**

Global Risks

JULY-DECEMBER 2021 ANALYSIS

Global Highlights: July-December 2021

Transactions

+44% ▲ Global transaction volume year-over-year (YOY)

+52% ▲ Financial services transactions

+29% ▲ Ecommerce transactions

+45% ▲ Communications, mobile and media transactions

-10% ▼ Gaming and gambling transactions

Human-Initiated Attacks

+1% ▲ Human-initiated attack rate YOY

+20% ▲ Financial services attack rate

-1% ▼ Ecommerce attack rate

-31% ▼ Communications, mobile and media attack rate

+50% ▲ Gaming and gambling attack rate

Automated Bot Attacks

+32% ▲ Automated bot attacks YOY

+10% ▲ Financial services bot volume

+32% ▲ Ecommerce bot volume

+894% ▲ Communications, mobile and media bot volume

-58% ▼ Gaming and gambling bot volume

Global Transaction Patterns in Numbers

Mobile Accounts for 75% of all Events, as Login Volumes Explode

The relentless growth of online transactions continues with significant increases in logins as well as in payments. Global, accelerated digitalization, fueled by the pandemic, continues across a multitude of different demographics and geographies.

A modest increase in new account creations reconfirms the shift away from building new consumer relationships with consumers, instead demonstrating brand loyalty to existing accounts established over the last 18 months.

While restrictions on visiting physical stores were lifted in many parts of the world, the continuing strong growth of online payments shows that consumer behavior has fundamentally changed. More payment options continue to enter the market globally as Buy Now Pay Later, cryptocurrency and peer-to-peer payment options have become increasingly fashionable.

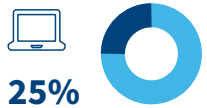
For the first time, three-quarters of all transactions were mobile, with the vast majority of those being initiated through an app. This can be attributed to many factors, such as more companies undertaking digitalization that includes a specific mobile app strategy, changing consumer preferences – driven especially by millennials and zillennials – and cheaper costs of mobile handsets and data around the world.

TRANSACTIONS PROCESSED JULY-DECEMBER 2021

35.5B ..... Growth YOY **+44% ▲**

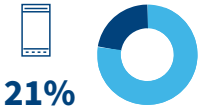
TRANSACTIONS BY CHANNEL

Desktop / Mobile



25% **75%** ..... Growth YOY **+9% ▲**

Mobile Browser / Mobile App



21% **79%** ..... Growth YOY **+10% ▲**

TRANSACTIONS BY USE CASE

		Growth YOY
New Account Creations	516M	+4% ▲
Logins	25.7B	+51% ▲
Payments	5.9B	+35% ▲

LexisNexis® RISK SOLUTIONS

Global Attack Patterns in Numbers

Human-Initiated Attacks Rise for the First Time Since 2019, as Automated Bot Attacks Target Communications, Mobile and Media (CMM)

HUMAN-INITIATED ATTACKS

Attack rates on individual online transactions that typically return full digital identity profiling data have increased for the first time since 2019, with significant growth in mobile app attack rates.

ATTACK VOLUME

344M

Growth YOY **+46%** ▲

Attack Rate by **Desktop** / **Mobile**

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

+9% ▲

ATTACK RATE

		Growth/Decline YOY
Overall	1.1%	+1% ▲
Desktop	1.8%	+12% ▲
Mobile Browser	2.2%	-6% ▼
Mobile App	0.6%	+59% ▲

AUTOMATED BOT ATTACKS

High velocity automated attacks that typically mass-test stolen identity credentials on a particular use case originating from a machine or series of machines have specifically targeted the CMM industry.

ATTACK VOLUME

1.6B

Growth YOY **+32%** ▲

		Growth/Decline YOY
Financial Services	890M	+10% ▲
Ecommerce	275M	+32% ▲
CMM	310M	+894% ▲
Gaming and Gambling	46M	-58% ▼

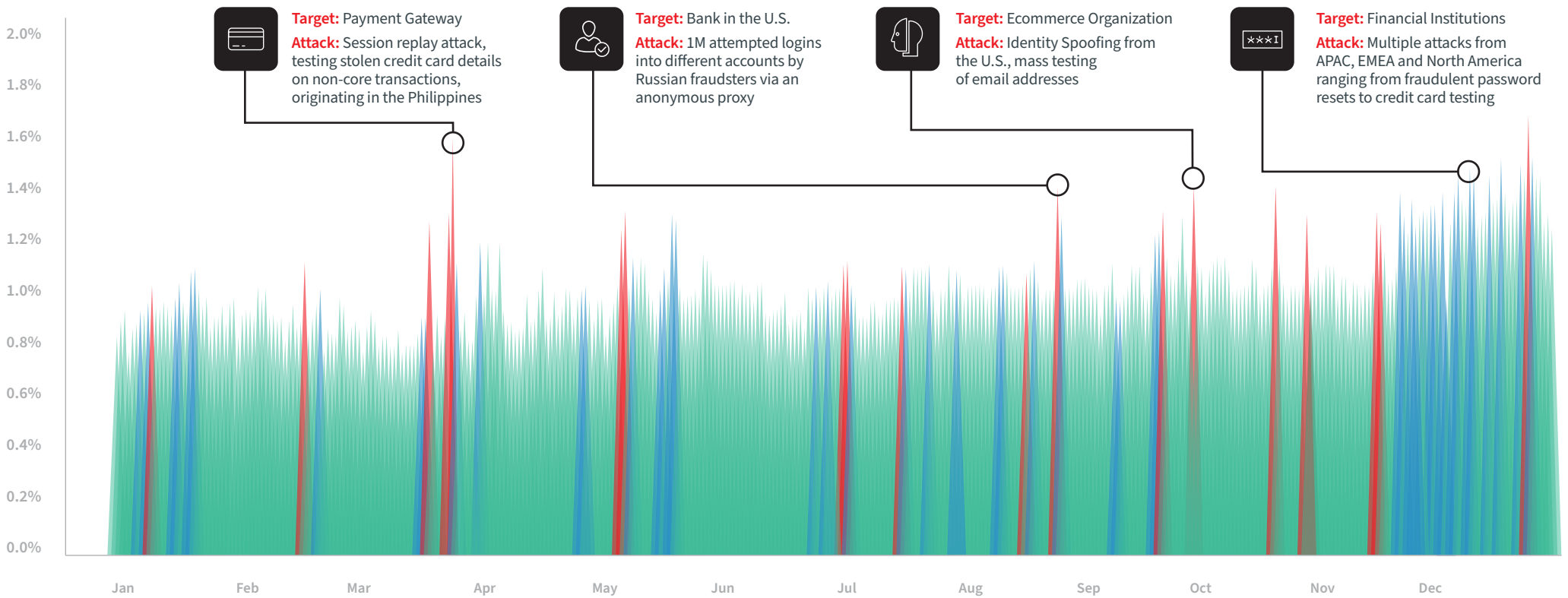
LexisNexis® RISK SOLUTIONS

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

Several Targeted Attacks Keep the Attack Rate Rising Throughout the Year

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 general trajectory of the index trends clearly upwards. The year ended with multiple attacks on financial institutions raising the Identity Abuse Index to its highest level.



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

The Rise of Mobile for Good Customers and Fraudsters

Desktop's Final Swan Song

In the first Cybercrime Report published in 2014, the percentage of mobile traffic in the Digital Identity Network was a mere 25%. In the second half of 2021, the mobile split of transactions reached 75% for the first time. The relentless shift to mobile continues, driven by younger generations embracing mobile technology earlier and earlier as well as emerging market populations skipping desktop devices altogether and moving straight to mobile services.

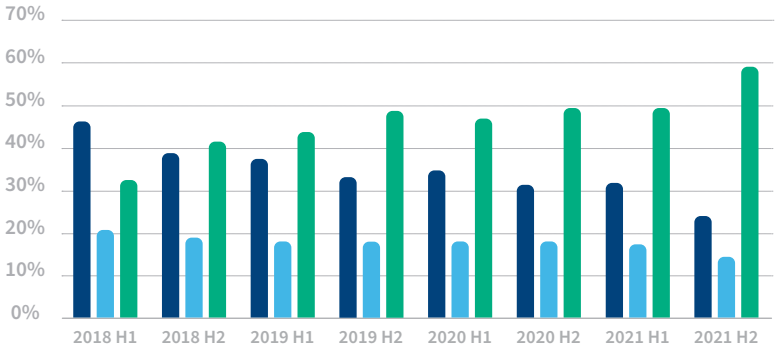
Looking at analysis of data from the last four years sourced from the Digital Identity Network, the decline of desktop transactions is clearly visible, as is the growth of the share of mobile app-based transactions – by far the most dominant transaction type in the second half of 2021. Interestingly, the share of mobile browser-based transactions has remained relatively stable, showing only a slight decline in 2021, reflecting a portion of the global population who may not have access to more sophisticated smart phones or who chose not to sign up to app-based services.

From an attack perspective, a similar shift has taken place. In the first half of 2018, the majority of attacks came via the desktop – even if mobile browser and mobile app attacks were combined. In the second half of 2021, even if the share of desktop attacks is still marginally in the lead, there is really little difference in the share of attacks across the three channels, as attacks have shifted significantly to mobile channels at the expense of the desktop channel.

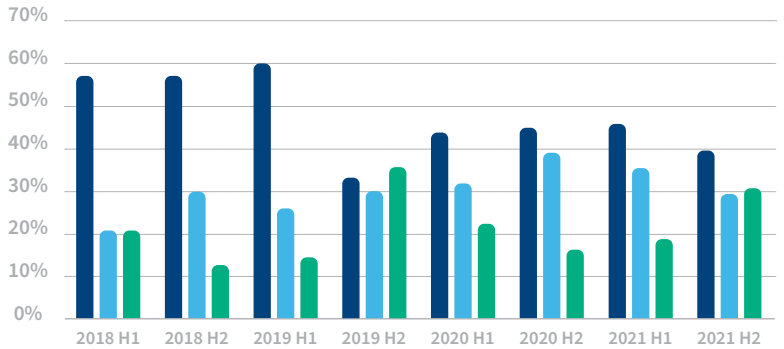
While potentially stronger security features of mobile apps can be a reassurance to organizations offering digital services, it is important to deploy multi-layer fraud prevention capabilities across all digital channels to be able to identify the anomalies associated with the growing number of attacks targeting the mobile app channel.

DESKTOP MOBILE BROWSER MOBILE APP

SHARE OF ***TRANSACTIONS*** ACROSS CHANNELS



SHARE OF ***ATTACKS*** ACROSS CHANNELS



LexisNexis® RISK SOLUTIONS

Fraudsters Leverage the Power of Networks to Facilitate Attacks

Hyperconnected Networks Continue to Target Multiple Industries and Organizations

The Digital Identity Network continues to record a strong pattern of cross-organizational, cross-industry and even cross-regional fraud.

It's likely that each network comprises several groups of fraudsters using the same lists of stolen identity data, which are being exploited across regions and industries.

Devices associated with confirmed fraud events are likely tied to the same individual or fraud ring, given that hardware is not shared in the same way as stolen data.

The analysis includes:

- The key links between dynamic digital identities, which join together devices and stolen identity data, including email addresses and telephone numbers.
- Transaction volumes that make up the fraudulent networks, to illustrate the size and scale of fraudulent behavior.
- The assigning of monetary values to the entire fraud network based on known payment transaction amounts.

The Digital Identity Network allows organizations to share intelligence related to confirmed fraud events so that an entity that is marked as high-risk or fraudulent by one organization can be blocked by subsequent organizations before further transactions are processed.

Uncovering Regional Networked Fraud Reveals the Close Links Between Financial and Telco Attacks

NETWORK IN NUMBERS

53,000+ Events

Were associated with the fraudulent digital identity

At least $2.4M

In fraud blocked

387,000+ Events

Recorded at other organizations in the Digital Identity Network that were associated with a digital identity that was involved in these original fraudulent events at source organizations

At least $10.3M

Was exposed to fraud across the entire network. Some of these transactions may have been blocked by organizations in the network who don't share fraud data.

See next page for network visualization

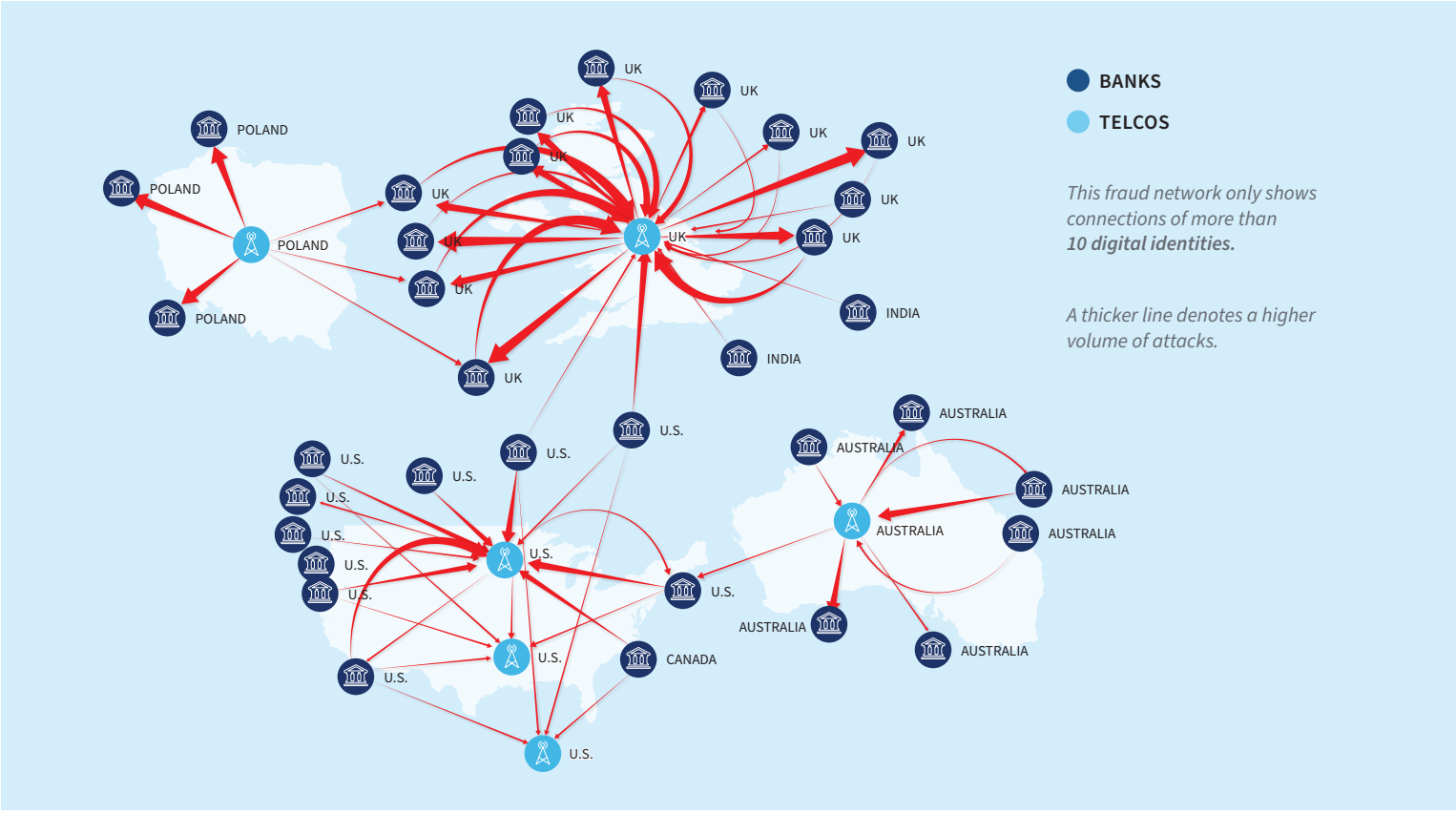
LexisNexis® RISK SOLUTIONS

Uncovering Regional Networked Fraud Reveals the Close Links Between Financial and Telco Attacks

This visualization shows regional fraud networks (linked by digital identity) targeting banks and mobile network operators during the second half of 2021. It also reveals links across regions, highlighting the truly global nature of fraud attacks.

As attacks on the financial sector become more complex, fraudsters will often initiate their attacks by obtaining new mobile phone contracts or taking over the accounts of existing wireless customers for use later in bank account takeover attempts or new account fraud. Analysis of the network shows that new account application fraud made up 44% of the attacks versus 56% account takeover fraud.

Each arrow illustrates digital identities associated with confirmed fraud attempts at one organization, crossing over to another organization in the Digital Identity Network. Cross-over occurs both ways: from banks to telcos as well as from telcos to banks. Links showing fraud attempts between banks have been removed for clarity.



The Life of a Prolific Fraudster

Fraud Attacks Across the Network from a Single Digital Identity

A FRAUDSTER IN NUMBERS

35 Organizations

Attacked by the same digital identity

580 Events

Were associated with the fraudulent digital identity

- **100** — Attempted account creations/credit card applications/loan applications
- **46** — Attempted ecommerce purchases
- **12** — Attempted password resets
- **7** — Attempted details changes

See next page for visualization

LexisNexis® RISK SOLUTIONS

The Life of a Prolific Fraudster

Fraud Attacks Across the Network from a Single Digital Identity

While the Digital Identity Network can reveal the global nature of fraud networks, it is equally powerful at highlighting the prolific nature of some individual fraudsters at work.

The schematic shown here reveals only a part of the activity of one fraudulent digital identity during the second half of 2021. An initial attempt to apply for a new wireless contract at a telco operator was swiftly followed by numerous applications for new bank accounts and lines of credit across several financial organizations.

Several ecommerce purchase attempts were then made at a variety of online jewelry stores, before focusing on account takeover at financial institutions, with several password reset attempts across different accounts and finally, an online enrollment account takeover attempt at an insurance company.

As fraudsters continue to benefit from breached identity data and automated bot credentials testing, the ability for organizations to benefit from global shared intelligence enables them to identify and stop more attempted fraud in near real-time.

The Global Scam Pandemic: Attacks and Defenses

The last 12 months have seen scams of various kinds growing into a global pandemic, with governments, financial institutions and citizens around the world looking for solutions.

Modern day scammers operate much like a business entity with highly efficient digital skills, processes, and wide-ranging teams. Although most prominent scams trick money out of victims' bank accounts, scammers are industry agnostic and often target different industries such as social media to harvest personal information ahead of the actual scam. Phishing and smishing are increasingly common launch pads for the information gathering stage of a scam attack, while automated bots can be used to validate compromised usernames and passwords available on the dark web.

In order for a scam to be a success, the fraudster needs to gain access to an account – either directly or through manipulating the victim to access their account and move money out themselves. Frequently, a second factor of authentication such as a one-time password sent by SMS, push notification or email is obtained by the fraudster to facilitate account access and money transfer. Entered unwittingly by the victim on a phishing site mimicking the real bank's website, or given up voluntarily as part of an elaborate entrapment story, this one-time password is the keys to the kingdom, enabling the fraudster to change email or phone details, register their own phone as a soft token and define new beneficiaries for the final act of their sad story.

Whichever way the money is moved out of the victim's account (by themselves or by the fraudster), a mule account must be available to receive the funds. Aggressive recruitment of mules is widespread, although the rapid shift to digital during the covid pandemic has also enabled cybercriminals to open fraudulent accounts using stolen or synthetic identities – hiding among the large volumes of genuine customer applications. Once transferred, the money is rapidly transferred in smaller amounts around the global mule network, taking advantage of the world's expanding rapid payment systems to disappear swiftly and without a trace.

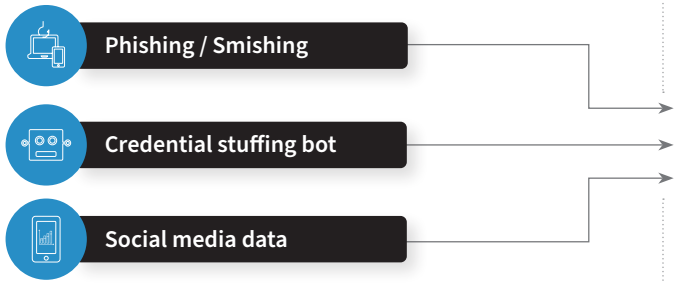
⚠ See next page for visualization

LexisNexis® RISK SOLUTIONS

The Global Scam Pandemic: Attacks and Defenses

Breaking a Scam Down into its Three Stages can Reveal Opportunities to Mitigate the Risk

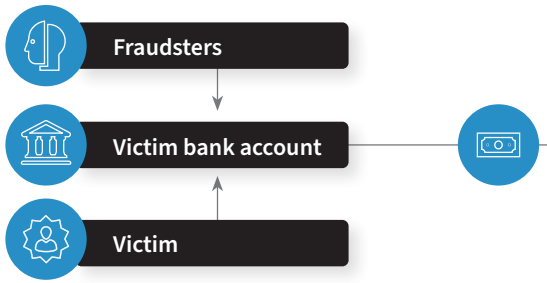
INFORMATION GATHERING



User credentials and personal information leaked from data breaches are harvested and traded on the dark web. Users can still take steps to ensure they rotate passwords on a regular basis and ensure they don't succumb to phishing attacks which have re-emerged as a significant threat in 2021. Education is key, especially for new digital users, to ensure that they are aware of the risks of clicking on links in emails and SMSs.

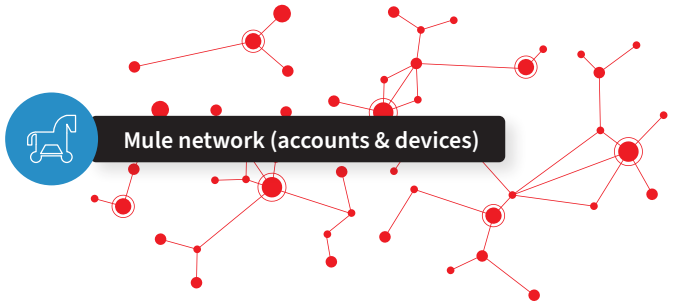
Technological defenses are required – both to identify credential stuffing attempts and highlight potential accounts at risk. Proactive services, which can attempt to neutralize bots as well as take down phishing sites imitating real service providers, are also required.

ACCOUNT ACCESS



With millions of payments happening every day around the world, the challenge is to find the anomaly that identifies an account access associated with a scam payment. Data is key here – being able to understand historical transaction history for an account, in combination with the rich digital intelligence that identifies the usual device, location and behavior associated with account access, together with any active threats. Sophisticated analytics, operating in near real-time, which look across the full user journey – not just the moment of payment – together with the ability to consider global intelligence, will help reduce false positives and target the key anomalies that need to be reviewed.

CASH OUT



Once money has been transferred from one bank to another, or across international borders, it is very difficult to get that money back. Cybercriminals have no such constraints. A robust solution for scams requires a proactive attack on money mules and their accounts. Real-time analytic models have been shown to be effective in identifying mule accounts. Layering payment account data with digital intelligence provides a unique multi-dimensional set of data to establish links between mules. Combining this with a collaborative approach to reporting mule accounts via consortiums will enable a near real-time mule detection defense that makes it more difficult for fraudsters to take advantage of their scam victims' accounts.

Across the Customer Journey

JULY-DECEMBER 2021 ANALYSIS

Customer Journey Highlights: July-December 2021

New Account Creations

1 in every 10 account creations are attacks

77% YOY growth in bot attacks

.

Logins

Highest volume growth across all core use cases

138% YOY growth attack rate on mobile app logins

Payments

Highest volume of attacks across all use cases

63% YOY increase in volume of mobile attacks

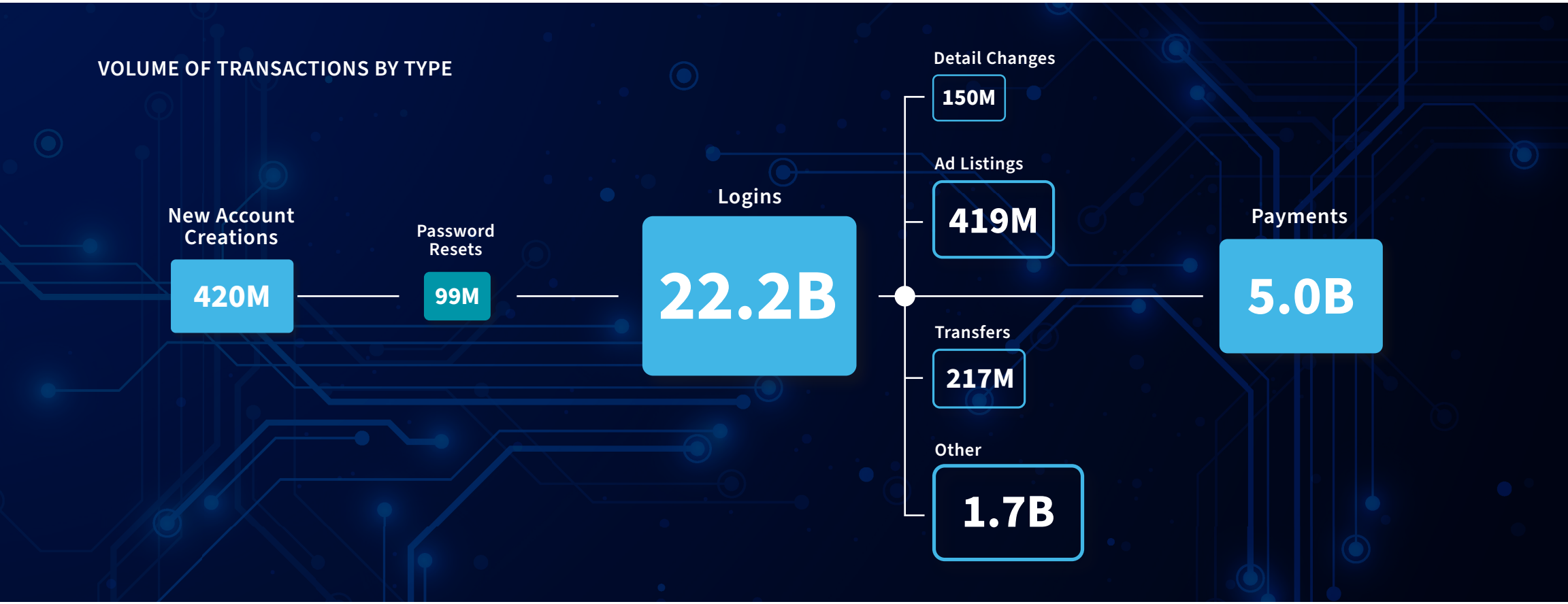
Password Resets

1 in every 8 password resets are attacks

LexisNexis® RISK SOLUTIONS

Volume of Transactions by Use Case Across the Online Journey

Profiling Risk Across Each Customer Touch Point



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 Touch Points

Risk Increases Across All Three Core Use Cases

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	The growth in volume of new account creations continues to slow after significant growth at the start of the pandemic. However, the risk associated with digital onboarding remains, with almost 1 in every 10 events being an attack. Automated bot volumes targeting new account creations have grown by 77% YOY.	Empowered consumers accessing the wealth of digital services now offered globally drove up login volumes 51% YOY. Fraudsters continue to shift their attention to account takeovers, with login attacks via mobile apps up 138%, while the overall login attack rate grew at 24%.	Payment attacks enable fraudsters to monetize their work by cashing out quickly and efficiently. The payment mobile app attack rate grew fastest, at 57% YOY, while the overall payment attack rate grew at 8%.
ATTACK RATE			
OVERALL	9.0%	0.5%	3.2%
DESKTOP	**13.3%**	**1.0%**	**3.7%**
MOBILE BROWSER	9.3%	0.6%	3.4%
MOBILE APP	3.0%	0.3%	2.6%

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

One in Four Password Resets on Desktop Are Attacks

	PASSWORD RESETS	DETAIL CHANGES	AD LISTINGS	TRANSFERS	OTHER
RISK TRENDS	Password resets are the highest risk touch point for the first time this period, with attack rates rising sharply on both mobile app and desktop. Weak password reset controls can enable a fraudster to quickly gain access and lock a victim out of their account, enabling the fraudster to withdraw money or make purchases.	Fraudsters change email addresses and mobile numbers to one they control to bypass security methods such as an SMS one-time password (OTP). Attack rates on details changes touch points declined significantly 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. Attack rates remained relatively stable YOY.	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 dropped significantly YOY.	Encompassing several other high-risk touch points such as new channel registration, standing order mandates, direct debits and beneficiary modifications. Attack rates associated with other touchpoints dropped significantly YOY.
ATTACK RATE					
OVERALL	12.8%	0.9%	0.5%	0.4%	1.0%
DESKTOP	**24.6%**	0.9%	0.6%	**0.9%**	**1.6%**
MOBILE BROWSER	1.7%	0.8%	**1.0%**	0.4%	1.0%
MOBILE APP	3.1%	**1.1%**	0.5%	0.3%	0.6%

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.

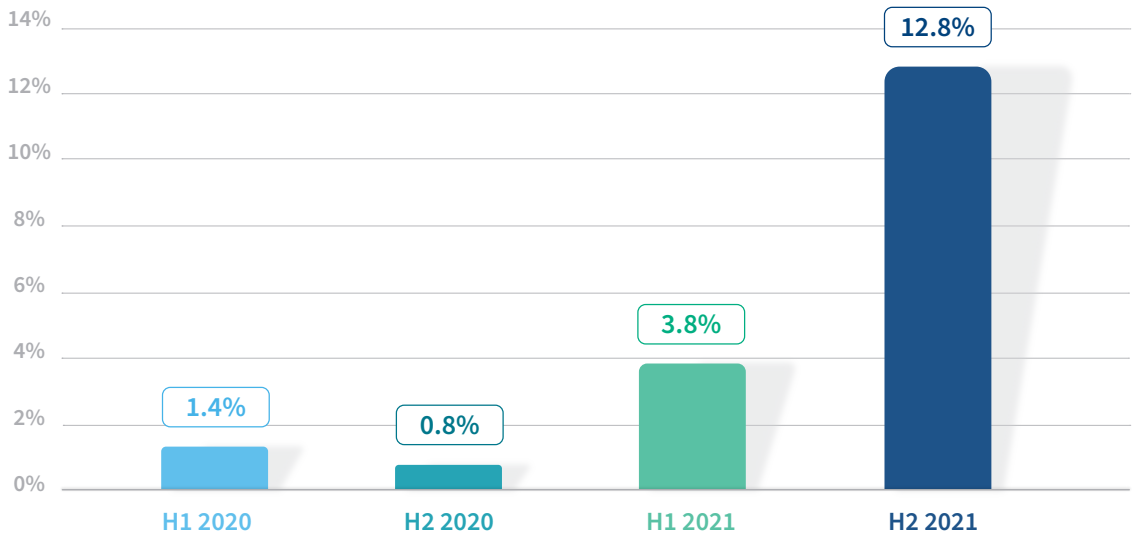
Password Reset – A New Focal Point For Fraud

Attack Rates Jump as Digital Accounts Come Under Attack

The ability to reset your password online is both a convenient feature for consumers who struggle to manage their ever-growing list of digital accounts, but also a key area of opportunity for cybercriminals. The ability to fraudulently reset a password can lock genuine users out of their account, leaving the fraudster to take over control.

With the creation of new accounts online having exploded during the last two years, fueled by the pandemic and the global shift to digital, fraudsters are now setting their sights on these new accounts. The growth in attacks on password reset functionality has accelerated, with one in eight password reset attempts now an attack, compared to less than one in fifty back in H1 2020.

PASSWORD RESET ATTACK RATE



See next page for password reset visualization

Password Reset – A New Focal Point For Fraud

Attack Rates Jump as Digital Accounts Come Under Attack

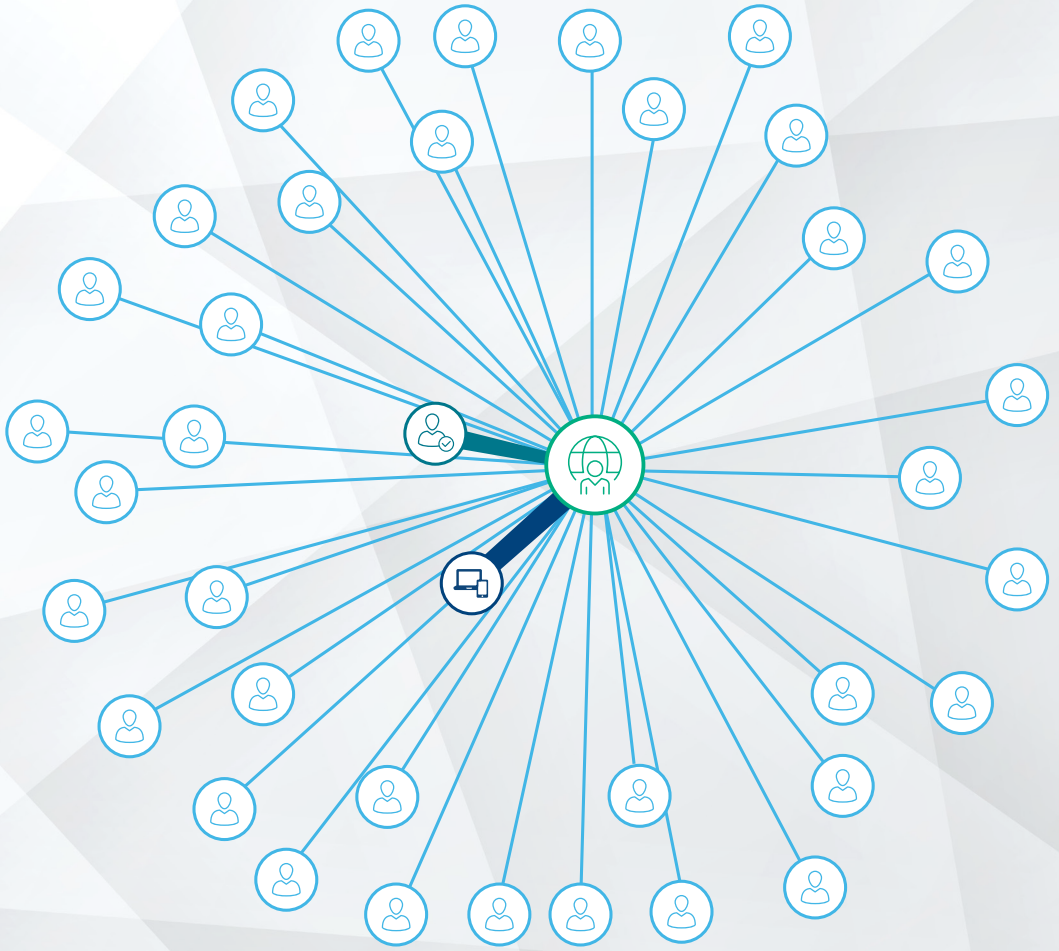
One unique LexID® Digital entity indicates a single source of password reset abuse attacking multiple accounts. All events came via a hidden proxy, with the digital identity pretending to be in the U.S. while actually located within China.

LexID Digital

Account Login

Account Name

Device ID



LexisNexis® RISK SOLUTIONS

Regional Trends

JULY-DECEMBER 2021 ANALYSIS

Regional Highlights: July-December 2021

APAC

+90% ▲ transaction volume YOY

+5% ▲ human-initiated attacks YOY

+135% ▲ bot volume YOY

EMEA

+16% ▲ transaction volume YOY

+7% ▲ human-initiated attacks YOY

+16% ▲ bot volume YOY

LATAM

+473% ▲ transaction volume YOY

+138% ▲ human-initiated attacks YOY

+455% ▲ bot volume YOY

North America

+22% ▲ transaction volume YOY

+50% ▲ human-initiated attacks YOY

-7% ▼ bot volume YOY

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

Identity Abuse Index by Region

LATAM Volatility Continues as EMEA and North America Trend Upwards

APAC EMEA LATAM NORTH AMERICA

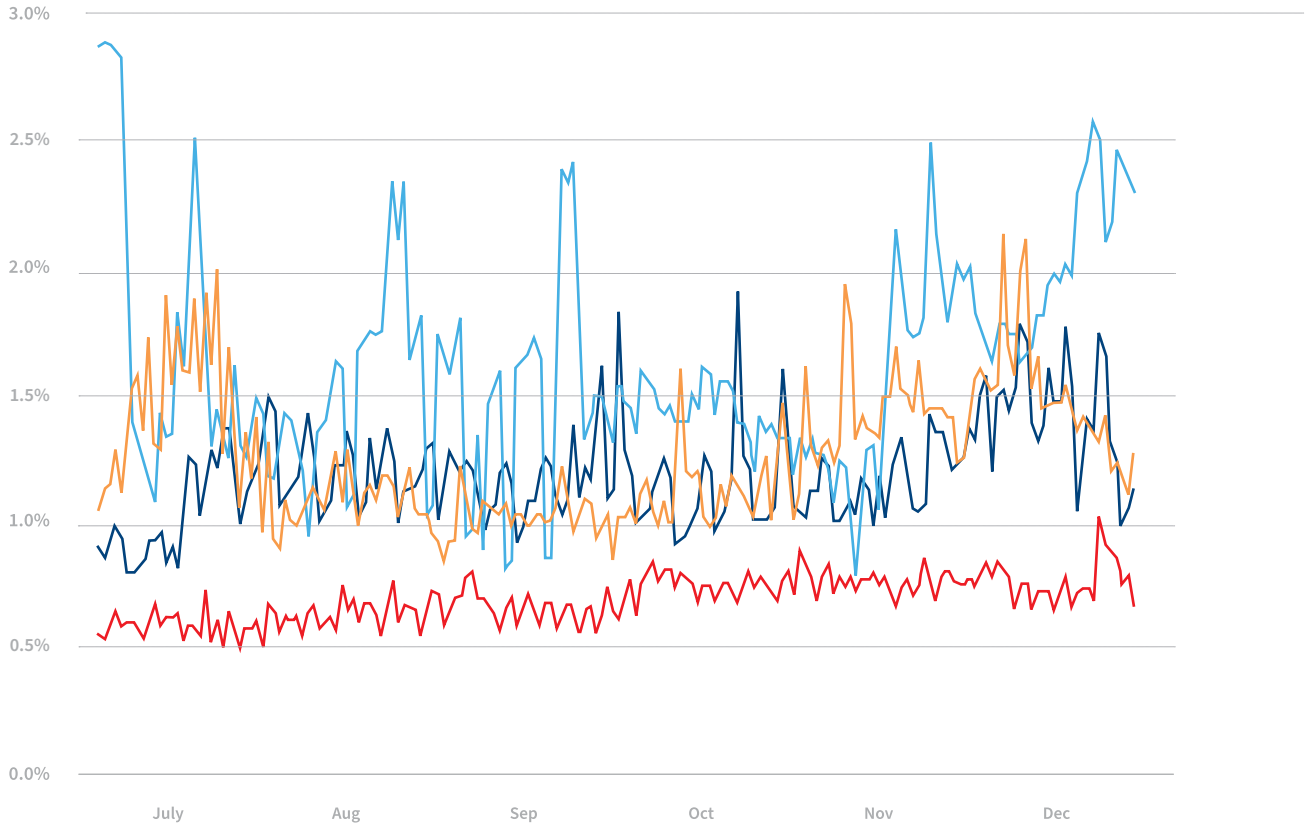
LATAM shows the most volatility across the regions, including several attack peaks throughout the second half of 2021, continuing as the highest overall attacked region.

APAC is the second most attacked region overall with peaks in July and November, although it saw a downward trend in attack rates through the whole of 2021.

North America continued the upward attack trajectory that was identifiable during the first half of the year, with attack rates appearing to trend upwards as the economy reopened.

EMEA continues with the lowest attack rates compared to other regions, however a clear upward trend is noticeable in the second half of 2021.

All regions apart from LATAM showed a year-end decline, possibly related to the emergence of Omicron and its associated impacts, including restrictions being reintroduced.



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 Continues To See a Large Increase in Bot Attacks

Neobanks, Cryptocurrency and BNPL Drive Transaction Growth

Emergence from restrictions appears correlated with increase in human-initiated attacks.

Asia-Pacific is home to 60%[1] of the world's population, with large parts historically being under-banked or unbanked (e.g, India, Bangladesh, Indonesia) and other parts being technologically and digitally advanced (e.g., Japan, Australia, Singapore). However, a great amount of effort has been undertaken by both the public and private sectors in providing low socio-economic and rural populations with a digital way to bank and pay, with the pandemic continuing to accelerate these efforts. Strong digital transaction growth continues to be seen across the region, with volumes up 90% year over year. This is explained by particularly strong uptake across a range of financial services such as neobanks, cryptocurrency exchanges and BNPL. Human-initiated attacks in the region have been on a downward trend since the start of the pandemic and this trend continued into the second half of 2021. Attack volumes did show an increase towards the latter half of the year aligned with loosening pandemic restrictions in many countries, before sharply dropping again in December as Omicron emerged. Only in gaming and gambling was a sharp rise in human-initiated attacks seen during the period. Automated bot attacks are the fraudster's primary attack vector in financial services, ecommerce and CMM, with bot volumes up 135% YOY.

APAC — especially Vietnam, Philippines, Singapore and Thailand — are among the global leaders in retail cryptocurrency investing. As retail investors continue to be attracted by the promise of high returns, governments are stepping in to regulate the cryptocurrency market amid the rise in crypto-focused scams as reported in the media. As human-initiated attack volumes start to rise again in the region, it is important for this industry to embrace the latest fraud prevention techniques and provide a level of reassurance to customers.

ATTACK SPOTLIGHT IN APAC JULY-DECEMBER 2021

Fraudsters from China aiming to freeze victims out of high-value financial institute accounts by targeting password resets.

Large automated bot attack on social media company targeting new account creations. Bots primarily originating from Indonesia, India, Bangladesh, China and Thailand.

[1] *https://www.worldometers.info/geography/7-continents/*

APAC Transaction and Attack Patterns

TRANSACTIONS

TRANSACTIONS PROCESSED

3.1B

Growth YOY
+90% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**

27% 73%

Mobile Browser / **Mobile App**

20% 80%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

Growth YOY
+5% ▲

AUTOMATED BOT ATTACK VOLUME

Growth YOY
+135% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**

60% 40%

Percentage of attacks coming from mobile devices has **decreased YOY**
-16% ▼

LexisNexis® RISK SOLUTIONS

APAC Position Against Global Figures

APAC Falls Below Global Average for Mobile App Attack Rate, Keeps Above Average Position Across All Other Channels

	GLOBAL	APAC
OVERALL ATTACK RATE	1.1%	1.3%
DESKTOP ATTACK RATE	1.8%	2.8%
MOBILE BROWSER ATTACK RATE	2.2%	2.6%
MOBILE APP ATTACK RATE	0.6%	0.2%

APAC's overall attack rate is higher than the global rate. Overall attack rates and the mobile channels attack rates continue to fall, while desktop channel's attack rate rises, continuing to create a larger gap between APAC and global desktop attack rates.

The region continues to see enormous growth in automated bot attacks, with cases more than doubling in number. This is reflected in the global top 10 automated bot attack list, which includes Japan, India, Indonesia and Bangladesh.

EMEA Sees Lowest Overall Attack Rate, Driven by Mobile App

Trust in Genuine Customer Enables Companies to Focus on User Experience

The range of digital payment methods continues to grow across the diverse markets of EMEA, driven by emerging technologies or regulation. Standard Card-Not-Present transactions are joined by a growing number of direct from bank transfers, together with various BNPL offerings, mobile payments and payments via social media apps. More than half of all mobile payments in EMEA secured by the Digital Identity Network are now in-app payments. Across all digital interactions in the network from EMEA, 80% are mobile based. With the lowest attack rates across all regions, companies are able to focus on user experience, by building secure digital trust relationships with their customers through acting upon data in the Digital Identity Network.

While EMEA attack rates are historically low, the second half of 2021 saw growth in the volumes of both human-initiated and automated bot attacks, suggesting that the increased human-initiated attack rates seen in the U.S. as the economy reopened are starting to play out in EMEA too. This is partially offset in parts of EMEA by attack rates decreasing on payments due to the Strong Customer Authentication mandate from PSD2, with ecommerce merchants and issuers relying on 3DS2.x to add security and compliance within the payment process.

Attacks on logins from automated bots in the CMM industry are particularly prevalent with the aim to access accounts and mine information on their victims for potential targeted social engineering attacks in other verticals.

Digital transformation is at different stages across EMEA, from Western Europe to sub-Saharan Africa. This results in distinctly different levels of fraud awareness and fraud methodologies across the region. Particularly in Africa, as the region jumps into digitalized banking and payments – the attack vectors of smishing, phishing and vishing are predominant. The common theme in these attacks is that the fraudsters want access to the victim's details or wants the victim to pay them by tricking the victim into thinking they are from a genuine organization like the victim's own bank. Many of these attacks exploit Personally Identifiable Information available from data leaks or social media where fraud detection may be relatively weak, and use this to establish trust and convey a sense of realism and urgency.

ATTACK SPOTLIGHT IN EMEA JULY-DECEMBER 2021

- Identity and device spoofing attacks from Eastern Europe attempt account takeover on ecommerce marketplace login page.
- Attack from the UK on a financial institution, aiming for account takeover via password reset.

EMEA Transaction and Attack Patterns

TRANSACTIONS

TRANSACTIONS PROCESSED

10.1B

Growth YOY
+16% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**

20% 80%

Mobile Browser / **Mobile App**

21% 79%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

Growth YOY
+17% ▲

AUTOMATED BOT ATTACK VOLUME

Growth YOY
+16% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**

47% 53%

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

-6% ▼

LexisNexis® RISK SOLUTIONS

EMEA Position Against Global Figures

EMEA Continues to Have the Lowest Attack Rates Globally, However Desktop Attacks See Largest Growth

GLOBAL EMEA

Due to a generally mature digitalized environment with high volumes of trusted consumer interactions, together with emerging regulations around enhanced use of Strong Customer Authentication for digital payments, EMEA generally sees lower attack rates across the board compared to the global average. Attack rates declined 8% YOY, but actually grew by 11% compared to the first half of 2021 as economies reopened in the second half of the year.

The digital maturity of the European portion of the market also explains the relatively small growth in transaction volumes compared to other regions.

As more and more traffic moves to mobile, less sophisticated fraudsters continue to attempt to exploit desktop weaknesses, with EMEA experiencing the highest growth of desktop attacks at 13% YOY.

LATAM Takes First Place in Automated Bot Attack Volume Growth

Region Gets Comfortable with the Digital Economy

Latin American fintech revolution provides consumer choice, but becomes fertile ground for fraud.

The evolution in Latin America from brick-and-mortar shops and other services to the digitalized world is well and truly underway, accelerated significantly by the pandemic. With a record number of consumers accessing ecommerce platforms, opening digital bank accounts with ease and choosing from a multitude of payment solutions, the region has undertaken financial actions online rather than going to physical locations, in some cases many miles away from home or work.

The LATAM fintech and neobanking revolution is underpinned by the need to serve the large under-banked or unbanked population across many parts of the region. These emerging offerings, in combination with mobile handsets and data usage costs decreasing, have resulted in LATAM emerging as a truly mobile first region with 89% of transactions coming from mobile, of which 93% are initiated via mobile apps.

However, when populations get used to something new, their risk averseness can decrease. This is what is happening in LATAM. With the ease of opening new accounts and a plethora of ways to move money, fraudsters have fast caught on and realized that the LATAM digital market is fertile ground for committing fraud. LATAM is seeing a dramatic increase in both automated bot attacks and human-initiated attacks, the largest increase across all regions.

Fintechs and neobanks have seen a high customer acquisition rate across the region, and have also enjoyed high retention rates. These organizations should ensure strategic deployment of fraud prevention capabilities across the entire customer journey to combat the growing threat from attack. An incredible 800% increase in automated bot attacks at login during this period shows that fraudsters are coming after these existing customer accounts.

ATTACK SPOTLIGHT IN LATAM JULY-DECEMBER 2021

- Large automated bot attack in the CMM industry, leveraging mass credential stuffing to confirm valid stolen credentials that can be used in more sophisticated attacks.
- Password reset attacks from Brazil attempting account takeover at ecommerce sites.

LATAM Transaction and Attack Patterns

TRANSACTIONS

TRANSACTIONS PROCESSED

5B

Growth YOY
+473% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**

11% 89%

Mobile Browser / **Mobile App**

7% 93%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

Growth YOY
+138% ▲

AUTOMATED BOT ATTACK VOLUME

Growth YOY
+445% ▲

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**

28% 72%

Percentage of attacks coming from mobile devices has **decreased YOY**
-5% ▼

LexisNexis® RISK SOLUTIONS

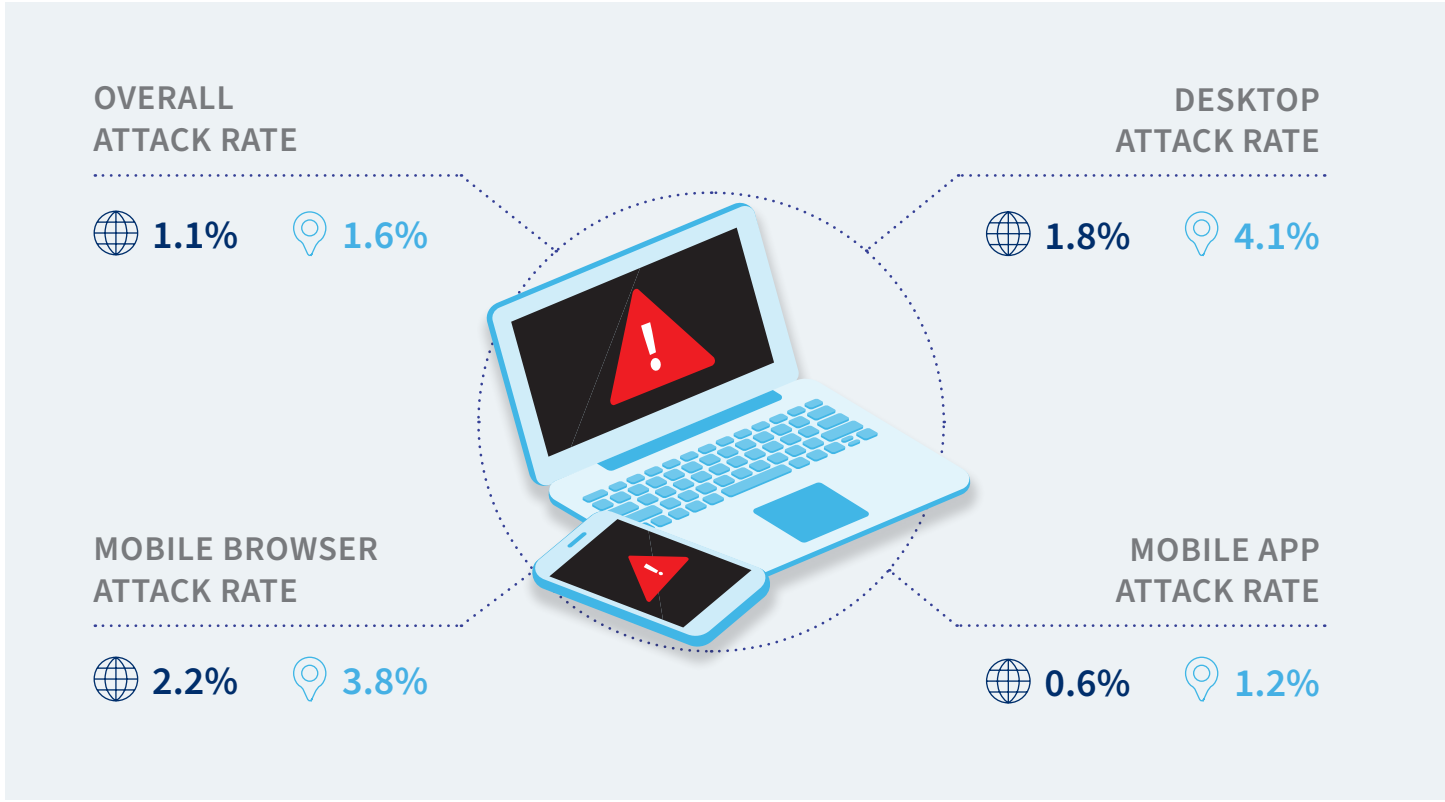
LATAM Position Against Global Figures

LATAM Maintains Top Position in Global Attack Rates

GLOBAL LATAM

The incredible growth in digital transactions (up more than 450% YOY) seen in the Digital Identity Network this period explains why the LATAM attack rate continues to decline in spite of more than 100% growth in attack volumes in the region. As a result, LATAM continues to occupy the top position across all four regions as fraudsters continue to attempt to exploit weaknesses in relatively new digital services across all channels, including desktop and mobile.

Automated bot attacks have shown the most growth in LATAM when compared across regions, targeting CMM and finance, with a strong focus on logins and password resets, as fraudsters target the accounts of customers who have been forced online during the pandemic.



Attack Rates in North America Increase as the Economy Reopens

Sophisticated, Human-initiated Attacks Dominate as Bots Take a Back Seat

The growing fraud trend that first appeared in the first half of 2021 has continued through to the end of 2021, albeit with quite some fluctuations in attack rates in the latter part of the year. Thanksgiving deals and the Christmas holiday period explain much of the fluctuation – this is prime season for fraudsters – as online shopping trends rise dramatically and fraudsters can hide among the legitimate high volumes of transactions. Especially during the latest Omicron strain, North Americans have increased their online shopping by spending their pent-up savings and stimulus checks and using more accessible credit methods available such as BNPL.

North America also appears to be following in Europe's footsteps and is experiencing a growing number of scam attacks. The media has reported a growing number of government grant scams, where fraudsters ask for checking account information or a one-off processing fee to deposit "government grant" money into the victim's account. Since the Omicron strain, this scam has been increasing. Investment scams, which are another type of Authorized Push Payment (APP) scam (where the victim transfers money to the fraudster) are also on the rise. With highly influential figures bringing cryptocurrencies into the mainstream on social media platforms, crypto investment scams trick victims into investing in cryptocurrency in promise of high returns. However, instead of any returns, the fraudsters disappear with the invested money. While it is not always possible to identify what type of fraud or scam is responsible for individual attacks seen within the Digital Identity Network, there is no doubt that fraud is on the rise.

With more and more U.S. states making legalized online gaming and gambling accessible, there is tremendous growth in the number of online gamers and gamblers and associated transaction volumes. This is reflected in the 34% increase in attack volumes seen in North America as fraudsters take advantage of this newly accessible industry.

ATTACK SPOTLIGHT IN NORTH AMERICAN JULY-DECEMBER 2021

- Large-scale attacks on a financial institution and ecommerce sites, targeting account takeover via password resets.
- Automated account creation attempts on a gaming and gambling platform originating from a hijacked guest WiFi service.

North America Transaction and Attack Patterns

TRANSACTIONS

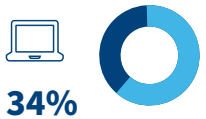
TRANSACTIONS PROCESSED

15.3B

Growth YOY
+22% ▲

TRANSACTIONS BY CHANNEL

Desktop / **Mobile**



34% 66%

Mobile Browser / **Mobile App**

28% 72%

ATTACKS

HUMAN-INITIATED ATTACK VOLUME

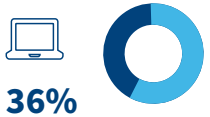
Growth YOY
+50% ▲

AUTOMATED BOT ATTACK VOLUME

Decline YOY
-7% ▼

HUMAN-INITIATED ATTACKS BY CHANNEL

Desktop / **Mobile**



36% 64%

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

+22% ▲

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

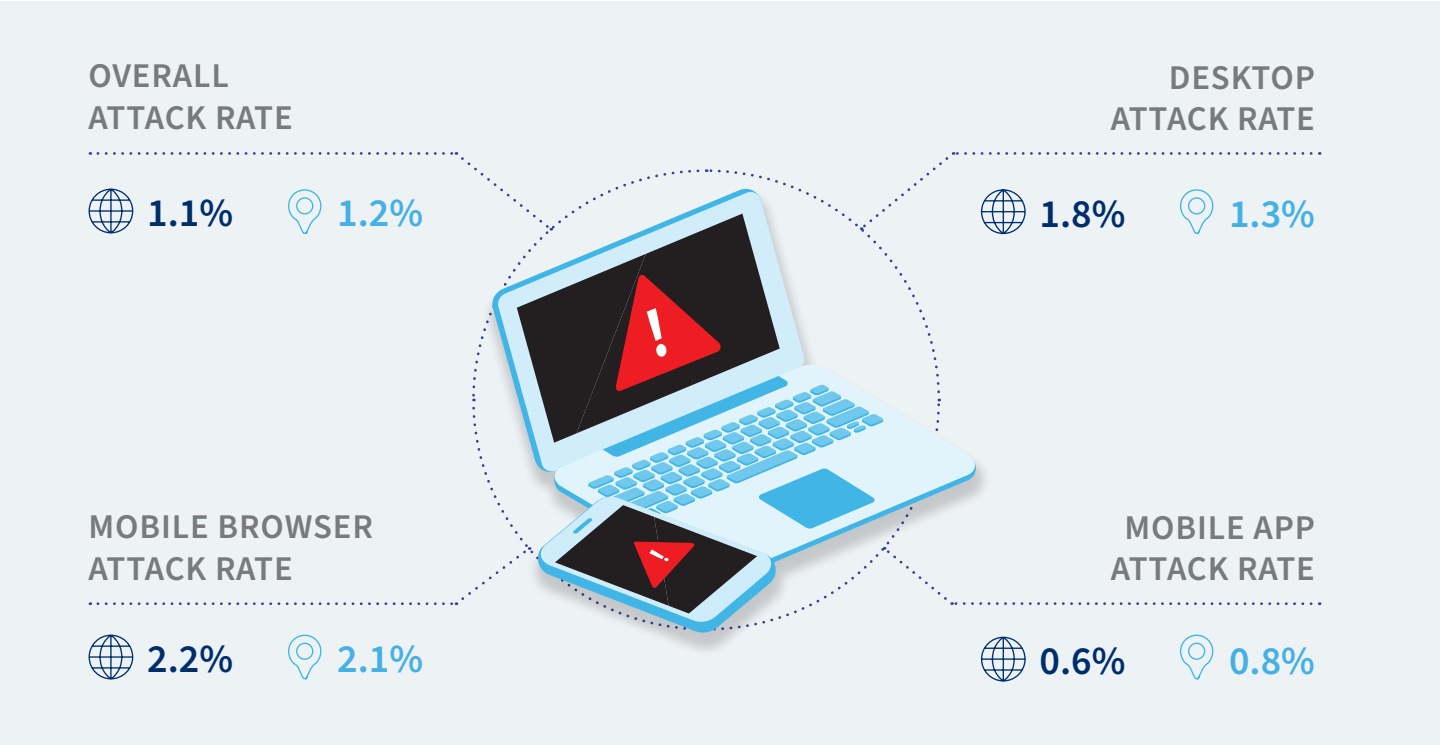
North America Position Against Global Figures

Fluctuating Daily Attack Rate Sees Several Small Peaks as North America Battles for Second Place on Global List

GLOBAL **NORTH AMERICA**

North America has seen a 20% increase in overall attack rate YOY, with a 42% increase compared to the first half of 2021. As the economy reopens after the pandemic, the attack rate in North America now moves above the global average. Attack rates in the mobile app channel specifically have seen significant growth up more than 300%.

The region saw a strong increase in human-initiated attack volume (up 50% YOY) but was the only region that saw automated bot attacks decrease.



Industry Opportunities

JULY-DECEMBER 2021 ANALYSIS

Industry Overview
Overview of Trends and Attack Patterns
Attacks Targeting Financial Services and Gaming and Gambling are on the Increase

INDUSTRY OVERVIEW	ALL INDUSTRY SUMMARY	FINANCIAL SERVICES	ECOMMERCE	COMMUNICATIONS, MOBILE AND MEDIA*	GAMING AND GAMBLING*
RISK TRENDS	Attack rates generally are increasing for the first time since 2019, with financial services and gaming and gambling leading the way.	Attack rates across financial services have increased, up 20% YOY and 41% compared with the first half of 2021.	Overall attack rates for ecommerce are stable although payment attacks continue to decline, especially in EMEA, attributed to the emerging SCA regulations there.	Although still having the highest attack rate by far, with fraudsters often focusing on industries such as social media and streaming platforms, CMM has seen a decline in attack rate of 31% YOY.	Following a prolonged period of significant bot attacks testing stolen credentials against the gaming and gambling industry, human-initiated payment attack rates have now risen significantly, with 146% growth YOY.
ATTACK RATE					
OVERALL	1.1%	1.0%	1.4%	5.3%	1.5%
DESKTOP	**1.8%**	**1.5%**	**2.3%**	3.9%	**1.7%**
MOBILE	0.9%	0.8%	0.9%	**6.0%**	1.5%

LexisNexis® RISK SOLUTIONS

** The historic Media industry classification used in previous Cybercrime Reports has now been split into two distinct industries – Communications, Mobile and Media and Gaming and Gambling.*
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
Attacks Focus on New Account Creations, as Mobile App Attacks Accelerate

The shift to mobile in financial services is a trend that has been accelerated by the introduction of digital banks around the world, generally providing an app-only interface to their customers. User experience is key, with digital banks fighting for customers and profitability, while legacy institutions search for their own path in the digitalized world. Correlating with lower costs for data and handsets around the world, the shift to mobile banking continues, with fraudsters following suit. Although the mobile attack rate remains low compared to desktop, it has grown at 26% YOY, as fraudsters continue to shift their focus to the mobile channel.

FINANCIAL SERVICES OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account creations saw the highest growth in attacks, up 73% YOY as fraudsters target fast and easy onboarding for digital banking.	Account takeover attempts are generally tiny in comparison to the sheer volume of good customer interactions occurring daily. In spite of this, login attacks were up 48% YOY, with mobile app attacks up more than 200%.	Financial services payment attack rates are generally the highest across all the industries reported on. Attacks were up 25% YOY, with mobile app attacks up more than 400%.
ATTACK RATE			
OVERALL	7.0%	0.4%	4.5%
DESKTOP	**11.5%**	**0.9%**	4.1%
MOBILE BROWSER	7.8%	0.5%	4.5%
MOBILE APP	2.8%	0.3%	**4.9%**

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
Online Merchants Pull Their Shutters Down on Payment Fraud

Economists say that the demand for goods and services drive economic growth after downturns. Consumers in every region have taken that to heart. We see the increase in online shopping being sustained even as the pandemic recedes and physical stores reopen. EMEA has led the way with 61% growth in payment transactions compared to the global average of 42% growth. As confidence in the world economy returned at the start of the second half of 2021, the success of new regulations in EMEA focused on reducing fraud was also apparent, with payment attack rates in EMEA down 35% YOY.

The accelerated shift to digital has driven merchants to commit to and fund their mobile app shopping experience. With increasingly easy methods for online payments and exclusive mobile app promotion deals, fraudsters are revising their attack vectors, with a noticeable rise in attacks on logins and new account creations via the mobile app, especially in North America and LATAM.

ECOMMERCE OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account creation attacks continue to grow, up 29% YOY, with growth across desktop and mobile channels. Desktop continues to be the preferred target vector, leading to every 1 in 8 transactions being an attack.	Mobile app attacks at login have almost doubled globally, as fraudsters catch on to the fact that many merchants now have a designated mobile app.	Ecommerce payment attack rates continue to decline, down 18% YOY, driven by declines in EMEA attributed to the ongoing roll-out of SCA in the payment journey due to PSD2 regulations. Payment attacks via mobile app showed the strongest decline, down 60% YOY.
ATTACK RATE			
OVERALL	6.7%	1.0%	1.9%
DESKTOP	**12.7%**	**1.4%**	**3.4%**
MOBILE BROWSER	4.5%	0.7%	1.6%
MOBILE APP	1.8%	0.5%	1.1%

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
Human-initiated Attacks Decline, Automated Bots Move In

CMM has long been the fraudsters' preferred industry to test stolen credentials. Historically, the likes of social media and streaming platforms tend to have a different balance between user experience and fraud prevention as they may not be as heavily regulated as financial institutions. The fraudsters' modus operandi is to test stolen credentials by logging in to existing accounts, for example, then validating which Personally Identifiable Information (PII) data is available to scam victims through other industry channels (such as banking) and committing APP scams. Validated credentials may then also be successfully used to hack into the victim's other accounts such as ecommerce apps. The ability to create new accounts using stolen or synthetic identities can also provide access to valuable services or handsets that can be resold for profit.

Human-initiated attack rates across CMM have declined throughout the pandemic and this trend continued through the second half of 2021, with only login attacks rates increasing slightly. As is often the case, when human-initiated attack rates decline, automated bots tend to increase. In this period a significant increase in automated bot attacks was observed, predominantly focused on credentials testing at login.

COMMUNICATIONS MOBILE AND MEDIA OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	The overall attack rate for new account creations in CMM continues to decline as has been the case since the start of the pandemic. Rates are however still higher than any other industry.	Login attack rate continues to be the highest overall across all industries and has held steady during this period. Attacks on desktop have seen a sharp rise, up 200%, however this has been balanced by significant decline in mobile app attacks (down 70% YOY).	CMM payment attack rates have declined by 31% YOY, driven by declines through the mobile channel.
ATTACK RATE			
OVERALL	12.9%	1.3%	2.1%
DESKTOP	**16.8%**	1.0%	**3.7%**
MOBILE BROWSER	12.2%	0.9%	2.0%
MOBILE APP	8.9%	**5.1%**	1.9%

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
Expanding Opportunities Drive Payment Fraud to New Highs

Deregulation in the gaming and gambling industry around the world has made consumers shift their paradigm to online betting and gaming platforms. Faster pay-outs, better gaming experiences and a non-evasive gambling process have facilitated repeat customer login to the platforms. Fraudsters have been waiting patiently in the wings, testing compromised or breached customer data through automated bot attacks during the pandemic.

Due to high market competition within the industry, gaming and gambling companies run bonus sign-on promotions with lower odds – enticing both genuine customers and fraudsters to take advantage. Although attack rates on new account creations are still high, during the second half of 2021 significant growth (100+%) in human-initiated payment attack rates were observed, while attacks on new accounts and logins declined.

GAMING AND GAMBLING OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Attacks on gaming and gambling new account creations declined by 15% YOY, although this still remains the most attacked point of entry as fraudsters take advantage of promotional schemes or look to money launder by creating multiple fraudulent new accounts.	Login attacks declined in the second half of 2021 as focus moved away from account takeover to cashing out from existing fraudulent accounts.	Payment attacks grew 146% YOY as fraudsters homed in on financial gains. Growth was primarily across desktop and mobile browser rather than app based.
ATTACK RATE			
OVERALL	8.0%	0.8%	2.1%
DESKTOP	**16.5%**	0.7%	**2.4%**
MOBILE BROWSER	6.5%	**1.0%**	**2.4%**
MOBILE APP	3.5%	0.2%	0.3%

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


Conclusion

Conclusion

The new year brings a certain optimism that in spite of (or even due to) Omicron, the world may finally be emerging from the pandemic and the global economy can continue to rebuild. Accelerated digital transformation acts as a great leveler both on a macro level (as emerging markets grow their economies to catch up with the developed world) and on a micro level (where unbanked, under-banked and under-serviced populations shift to digital for financial inclusion). The most successful organizations will be those that can provide a true omni-channel customer experience, addressing customer demand for great customer experience regardless where and when they interact, in combination with their latest smart phone.

Cybercriminals will be optimistic too. Never before has there been such a large attack surface available to them in the global digital world. The growth in phishing, as well as systematic testing of leaked Personally Identifiable Information via automated bot attacks, is already leading to a greater number of targeted scam attacks of all kinds, in all parts of the world. In a truly global digital economy, borders are no longer boundaries for trade or cybercriminals. Although digital onboarding remains the favored area of compromise for fraudsters, there is a clearly increasing focus on account takeover attacks, taking advantage of vulnerable consumers or insecure digital services.

Digital businesses will need to increasingly look to vendors that can bridge the gap between fraud prevention and excellent customer experience. Letting genuine customers interact without friction will be the key in customer retention. Stickiness within the mobile app will also drive upselling of products, revenue growth and profitability. Layered fraud prevention approaches will be needed that are flexible and adaptable, combined with broad digital intelligence from the customer journey, in order to provide protection to respond to emerging fraud vectors. Distinguishing between cybercriminals and good customers is no longer enough — identifying instances of risk that even the genuine customer may not be aware of is key.

It is more apparent than ever that fraud goes beyond single industries or countries. Businesses wishing to succeed in the digital world need to collaborate in the fight against fraud. This can be through taking advantage of the power of a global anonymized digital identity network, or even through the establishment of more focused digital consortiums among industry peers. It is time to unite in the fight against cybercrime.

Glossary, Methodology, Contact Details

Glossary

Industry Types

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

Fintech includes companies that use technology to make financial services more efficient with the goal of disrupting incumbent financial systems and corporations that rely less on software.

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

Communications, Mobile and Media includes mobile network operators, social networks, online dating sites and content streaming.

Gaming & Gambling include online gambling operators offering various betting options in regions where this is legalized.

Common Attacks

New Account Creation Fraud: Using stolen, compromised or synthetic identities, to create new accounts and 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 desktop computers received and processed by the 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 secirty control measures, and thus evade detection. These attafcks appear to be legitimate customer traffic, and they typically bypass truggers set around proticols and velocity rules.

LexID® Digital

LexID® Digital is the technology that brings Digital Identity Intelligence to life; creating a unique online identifier for every transacting user. This identifier is built using intelligence relating to devices, identity information, locations, behaviors, transaction details and threat data. LexID Digital helps businesses elevate fraud and authentication decisions from a device to a user level, as well as unites offline behavior with online intelligence. LexID Digital offers the following benefits:

- Bridges online and offline data elements for each transacting user.
- Goes beyond just device-based analysis and groups various other entities based on complex associations formed between events.
- Identifies a person irrespective of changes in devices, locations or behavior. Intelligence from the Digital Identity Network helps accurately recognize the same returning user behind multiple devices, email addresses, physical addresses and account names.

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 July – December 2021, during near real-time analysis of consumer interactions across the online journey, from new account creations to 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.

Fraud Network Linking

- Fraud performance data is taken from August to October 2021, based upon digital identities recorded as fraudulent in the Digital Identity Network.
- Monetary exposure is calculated on observed payment transactional value at risk from August to October 2021, based upon the identification of all transactions associated with that confirmed fraudulent transaction (and associated group of entities) during the period. It does not include any financial values at risk from customers who do not provide payment transactional data.

Data Processed and Analyzed

The overall volume of transactions processed by the Digital Identity Network July-December 2021 was 42 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 35.5 billion transactions.

The Cybercrime Report uses these 35.5 billion transactions to calculate overall transaction volumes globally and by region. There are 2 billion transactions without an IP address. These transactions cannot, therefore, be assigned to a region. They are mostly unknown sessions where an organization does not send the input IP address.

This subset of 35.5 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 30.2 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 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