



# REDEFINING TRUST AND RISK

## ADAPTING TO A POST-PANDEMIC WORLD

The LexisNexis® Risk Solutions Cybercrime Report  
January to June 2021

# 01 INTRODUCTION

## TABLE OF CONTENTS

01	FOREWORD .....	3
01	INTRODUCTION .....	4
<b>JANUARY-JUNE 2021 ANALYSIS:</b>		
02	Global Risks .....	5
03	Across the Customer Journey .....	21
04	Regional Trends .....	26
05	Industry Opportunities .....	41
06	CONCLUSION .....	54
07	GLOSSARY, METHODOLOGY, CONTACT DETAILS .....	56





# FOREWORD

JULIE CONROY | HEAD OF RISK INSIGHTS AND ADVISORY, AITE-NOVARICA GROUP

The COVID-19 pandemic is a black swan—a global phenomenon that has completely altered day-to-day reality for the majority of the population. Even now, more than 18 months since its inception, day-to-day commerce has not yet found an equilibrium point in the “new normal”. But amidst the continued uncertainty, there are a number of things we have learned over the course of the pandemic about good and fraudulent transactions that can help us chart our path forward as we ease back into some semblance of normalcy. Let’s start with a couple of key learnings about good customer behavior:

- **The pandemic put the pedal to the metal on digital transformation.** In-person options for banking transactions were restricted during the early days of the pandemic. Aite Group research shows that 39% of consumers tried a new digital financial product or service (e.g. online banking, mobile banking, person-to-person (P2P) transactions) during the pandemic, and the vast majority of these consumers intend to stick with these new behaviors post-pandemic.
- **Card-not-present (CNP) traffic continues to rise.** 2020 saw a spike in CNP volumes as consumers rapidly shifted in-person activities to CNP. The indications

year-to-date in 2021 are that consumers are also largely sticking with their digital-first behaviors for retail transactions as well, as evidenced by the continued rise in digital channel transactions from 1H 2020 to 1H 2021 shown in this report.

Of course, crime rings always capitalize on times of chaos and confusion, and the pandemic has brought ample servings of both. In 2021, the resumption of normalcy has come in fits and starts, as the pandemic continues to be a significant factor. Here are some of the ways in which fraud is manifesting for financial services firms across the globe:

- **The industrialization of fraud continues apace.** Organized crime rings continue to industrialize their attacks, leveraging mass data breaches, sophisticated automated tools, and deep dark-web intelligence. This is substantiated by this report’s statistics, which show that human-initiated attacks decreased by 29% YOY, while bot attacks increased by 41% YOY.
- **The analysis of consortium data highlights the extent to which these attacks are highly organized.** The value of the hive mind is invaluable in fraud mitigation. Organized crime rings do not attack any

single entity in isolation. The data in this Cybercrime Report clearly shows the value of consortium data in the fight against fraud, e.g. the 95,000-plus events recorded within the gaming and gambling verticals that had key digital identity data elements associated with confirmed fraud at other firms.

- **Attackers look for the weakest link in the chain.** Latin American firms have seen a sharp uptick in fraud. This is likely tied to the sharp uptick in digital activity related to COVID-19, while at the same time many of these businesses were not as well-protected against current attack vectors, representing lower-hanging fruit for crime rings.

As always, the LexisNexis® Risk Solutions Cybercrime Report is packed with insightful statistics regarding emerging attack vectors, as well as those that are tried-and-true. This should serve as a helpful compass to risk executives as they seek to navigate through this uncharted territory as we collectively work towards a return to some semblance of normalcy. Enjoy the read, and be safe and be well!

# INTRODUCTION

While many regions are still in the eye of the storm, fighting the most significant global pandemic of this generation, the seeds of optimism are growing. Navigating ongoing, emerging and uncertain conditions, businesses and consumers are looking towards rebuilding societies and economies.

As consumers have changed their behavior to adjust for large-scale restrictions to products and services, so too have fraudsters pivoted focus to continue to reap the benefits of cybercrime. Automation, identity spoofing, device spoofing, and social engineering have all grown in recent months as cybercriminals have identified their targets, and adjusted their attack profiles accordingly.

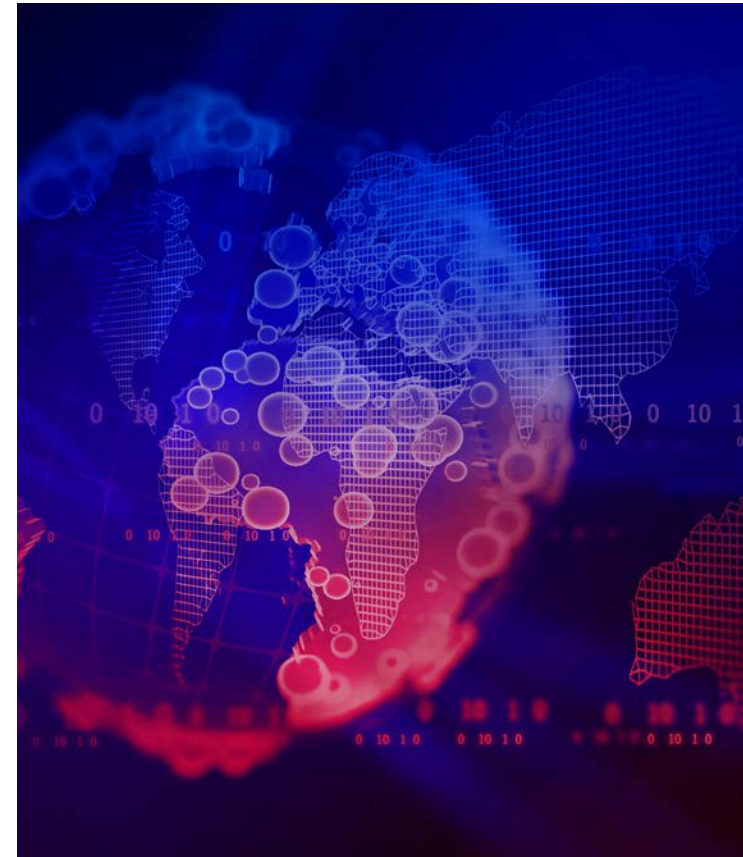
This pivot has manifested itself most clearly in the significant growth in bot volume targeting media organizations, testing stolen identity credentials on businesses that typically have fewer security layers to set up new accounts, or access existing ones.

Alongside this threat landscape, however, good customers continue to transact more, building trust with key merchants and organizations that they have come to rely on more than ever before. New platforms and ways of transacting have flourished, as users have embraced digital-only banks,

emerging payment methods such as buy-now-pay-later, as well as cryptocurrency investment options. Within the context of this rapidly evolving digital landscape, it has therefore become more critical than ever for digital businesses to ensure they are prioritizing low friction access to products and services without jeopardizing security.

## Key themes that will be explored further in this report include:

- The continued growth of good consumer transactions tempering the impact of fraud attack rates
- The patterns of changing consumer behavior as regions start to emerge from periods of lockdown
- The rise of automation: bot hotspots by region and industry
- The impact of networked fraud across different industries
- Industry spotlights on digital-only banks, buy now pay later and 3DS 2.x; as well as key digital transformation challenges facing the insurance industry





JANUARY-JUNE 2021 ANALYSIS: GLOBAL RISKS

02

JANUARY-JUNE 2021 ANALYSIS:

**GLOBAL RISKS**

# GLOBAL HIGHLIGHTS: JANUARY-JUNE 2021



## TRANSACTIONS

**+28%** ▲  
**growth** in global transaction volume year-over-year (YOY):



**+30%**  
**growth** in financial services transactions.



**+21%**  
**growth** in ecommerce transactions.



**+27%**  
**growth** in media transactions.



## HUMAN-INITIATED ATTACKS

**-29%** ▼  
**decline** in human-initiated attack rate YOY:



**-28%**  
**decline** in financial services attack rate.



**-27%**  
**decline** in ecommerce attack rate.



**-41%**  
**decline** in media attack rate.



## AUTOMATED BOT ATTACKS

**+41%** ▲  
**growth** in automated bot attacks YOY:



**+28%**  
**growth** in financial services bot volume.



**-9%**  
**decline** in ecommerce bot volume.



**+174%**  
**growth** in media bot volume.



# GLOBAL TRANSACTION PATTERNS IN NUMBERS

## Digital Payments Continue to Soar as Consumers Shift Further Online



Online transactions have continued their upward trajectory, with particularly strong growth recorded across logins and payments, indicating that consumers are relying on existing relationships with trusted brands more than ever before.

New account creations have predictably declined a little. This is due to the fact that the volume of new accounts peaked during the first few months of the pandemic, as consumers were moving their purchasing to online channels. This shift has now slowed as existing relationships are capitalized on as shown by an increase in logins.

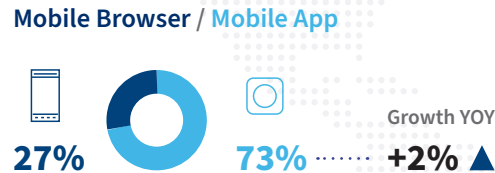
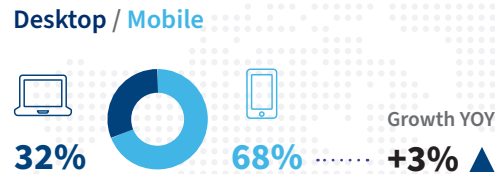
The online payment market continues to proliferate and diversify, with buy-now-pay-later (BNPL) services and digital wallets becoming increasingly popular ways to pay. This growth is likely to continue to cater for the growing population of consumers who are transacting more online.

Consumers are also continuing to shift to mobile in favor of desktop, with a strong preference for transacting via the security of a mobile app.

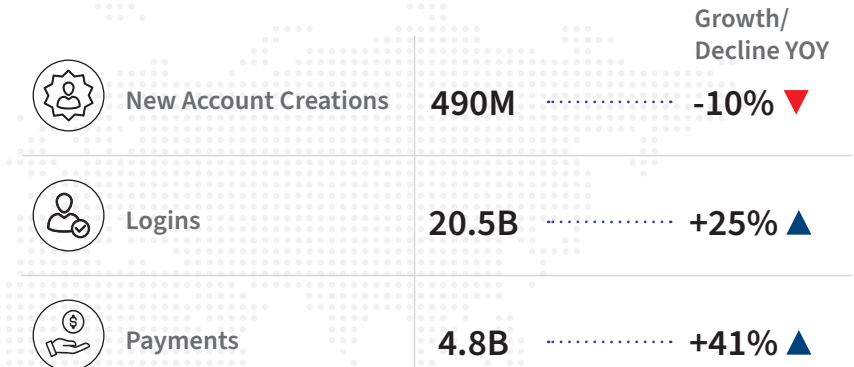
### TRANSACTIONS PROCESSED JANUARY-JUNE 2021



### TRANSACTIONS SPLIT BY CHANNEL



### TRANSACTIONS SPLIT BY USE CASE\*





# GLOBAL ATTACK PATTERNS IN NUMBERS

Human-Initiated Attacks Continue to Decline, While Automated Bot Attacks Targeting Financial Services and Media Grow



## 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 grown across financial services and media organizations in the LexisNexis® Digital Identity Network®.



## HUMAN-INITIATED ATTACKS

Attacks on individual online transactions, that typically return full digital identity profiling data, continue to decline across the Digital Identity Network®.

### ATTACK VOLUME

**1.2B**

Growth YOY  
**+41% ▲**



Financial Services

**683M**

Growth/  
Decline YOY  
**+28% ▲**



Ecommerce

**189M**

**-9% ▼**



Media

**351M**

**+174% ▲**

### ATTACK VOLUME

**236M**

Decline YOY  
**-9% ▼**

#### Attack Split by Desktop / Mobile



**46%**



**54%**

Percentage of attacks coming from mobile devices has decreased YOY



**-4% ▼**

### ATTACK RATE



Overall

**1.0%**

Decline YOY

**-29% ▼**



Desktop

**1.4%**

**-21% ▼**



Mobile Browser

**1.8%**

**-24% ▼**



Mobile App

**0.4%**

**-45% ▼**

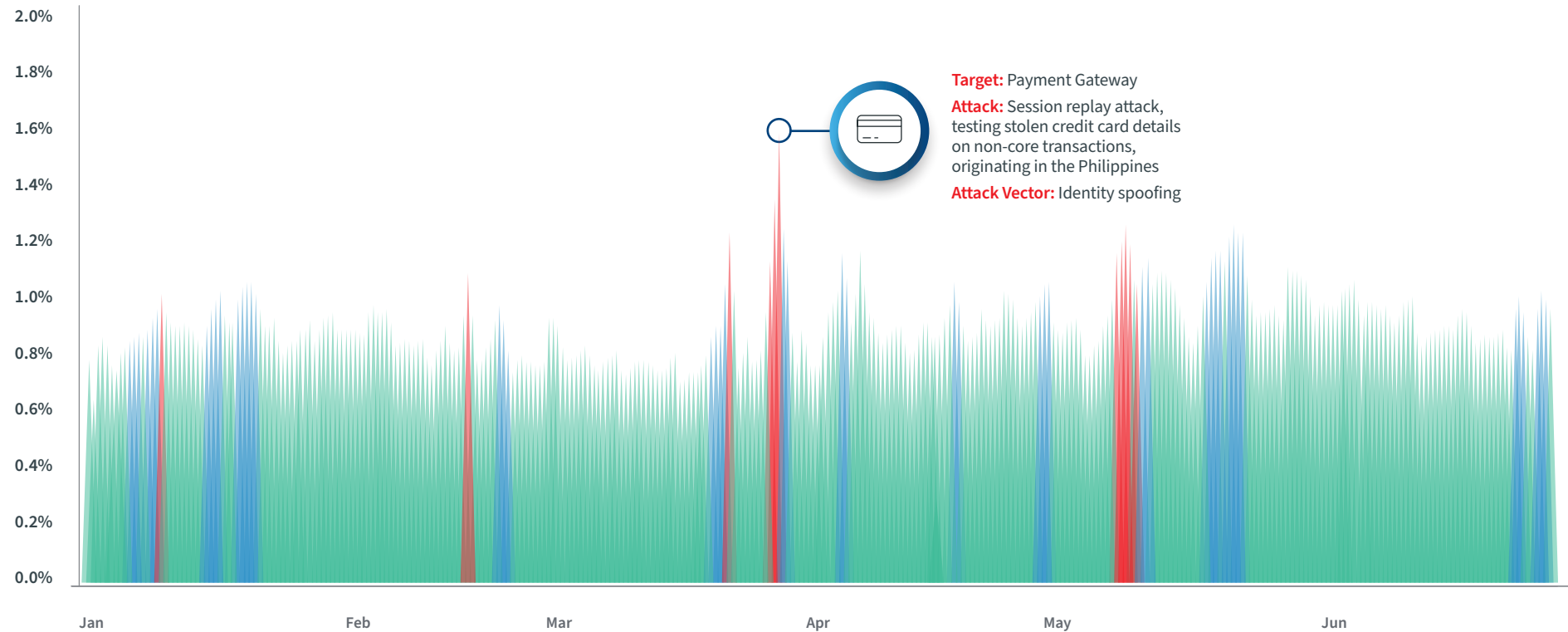
# IDENTITY ABUSE INDEX

## Large Identity Testing Attack from Philippines Targets Payment Gateway

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 attack rate was largely stable across the period, with some elevated bot activity during March, and a slight uptick in attack rate March through May.

### IDENTITY ABUSE INDEX

● LOW ● MEDIUM ● HIGH



# UNDERSTANDING THE RISK OF STOLEN EMAIL ADDRESS DATA

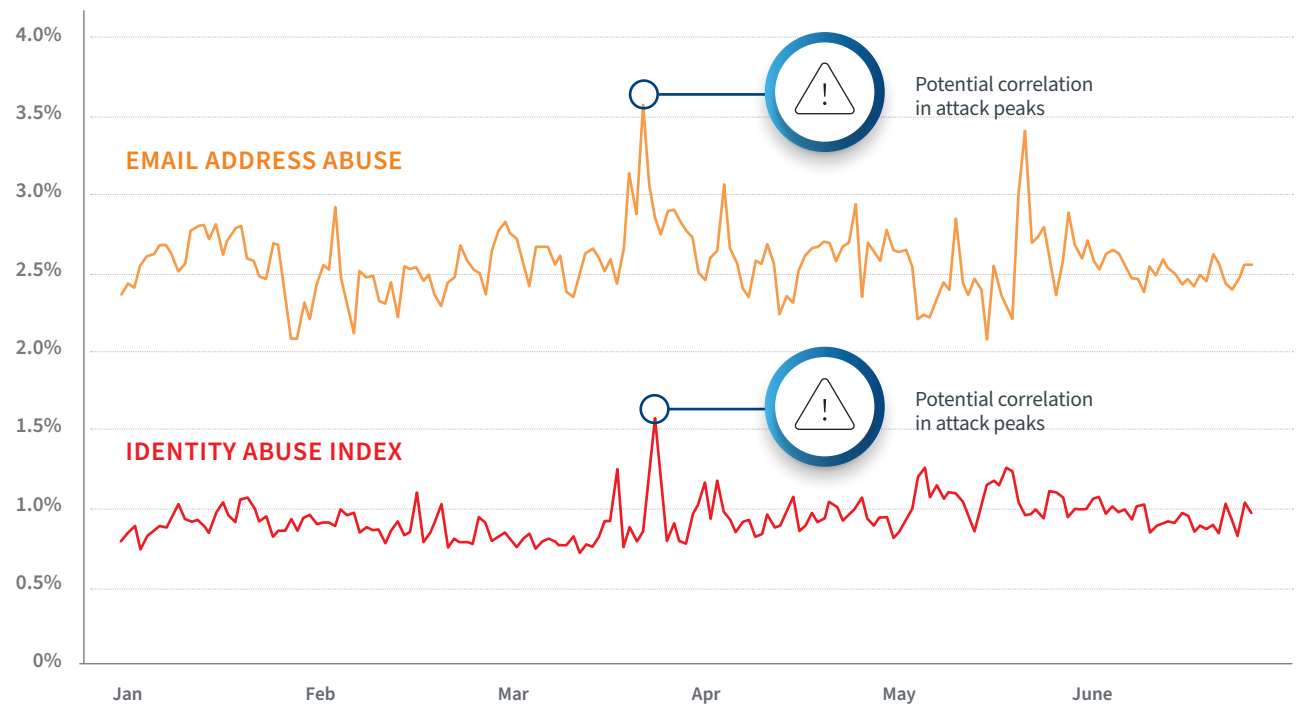
## Overlaying Email Address Abuse onto Daily Attacks Highlights Correlation of Stolen Data

Tracking the percentage of attacks, per day, across the Digital Identity Network gives organizations a clear view of peaks and troughs in identity abuse.

By overlaying email address abuse data, organizations can build an enhanced view of risk.

Comparing peaks in fraud attacks and email address abuse suggests a correlation in the usage of stolen credentials, likely following a specific data breach or fresh availability of stolen identity data.

### OVERLAYING THE IDENTITY ABUSE INDEX WITH EMAIL ADDRESS ABUSE

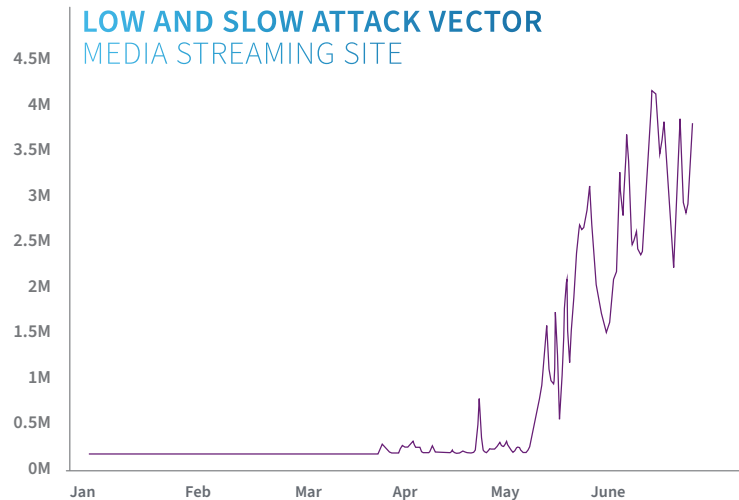




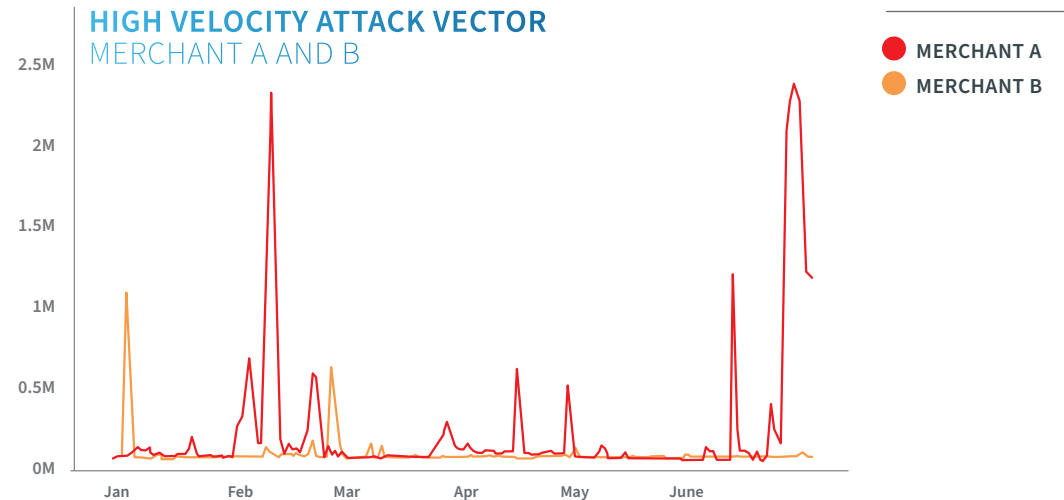
# AN ANALYSIS OF ACCOUNT TAKEOVER BOT TYPOLOGIES

## From Low and Slow Stealth Attacks to Short Sharp Volume-Based Approaches

Automated bot attacks use extensive attack typologies to trick or overwhelm business fraud defenses. The charts below detail examples of stealth attacks that build up over a series of months to short, sharp high velocity attacks that are conducted over a series of days.



- This series of **email testing bots attempting account takeovers**, was targeting logins at a media streaming site. The bots began testing low volumes in March, ramping up to 4.3M bots per day by the end June.
- The first period recorded a few hundred thousand bots coming from Italy, Portugal and Germany, then 25M from Spain and recently 35M from Japan.
- The bot has tested a total of 59M email addresses since March.



- These short, high velocity bot attacks targeted a series of ecommerce merchants in North America across defined two or three-day periods.
- They were predominantly attempting **account takeovers**, testing stolen identity credentials to login to good user accounts.
- At times, these bots made up 80% of a merchant's daily traffic.

# LARGEST ORIGINATORS OF AUTOMATED BOT ATTACKS, BY VOLUME

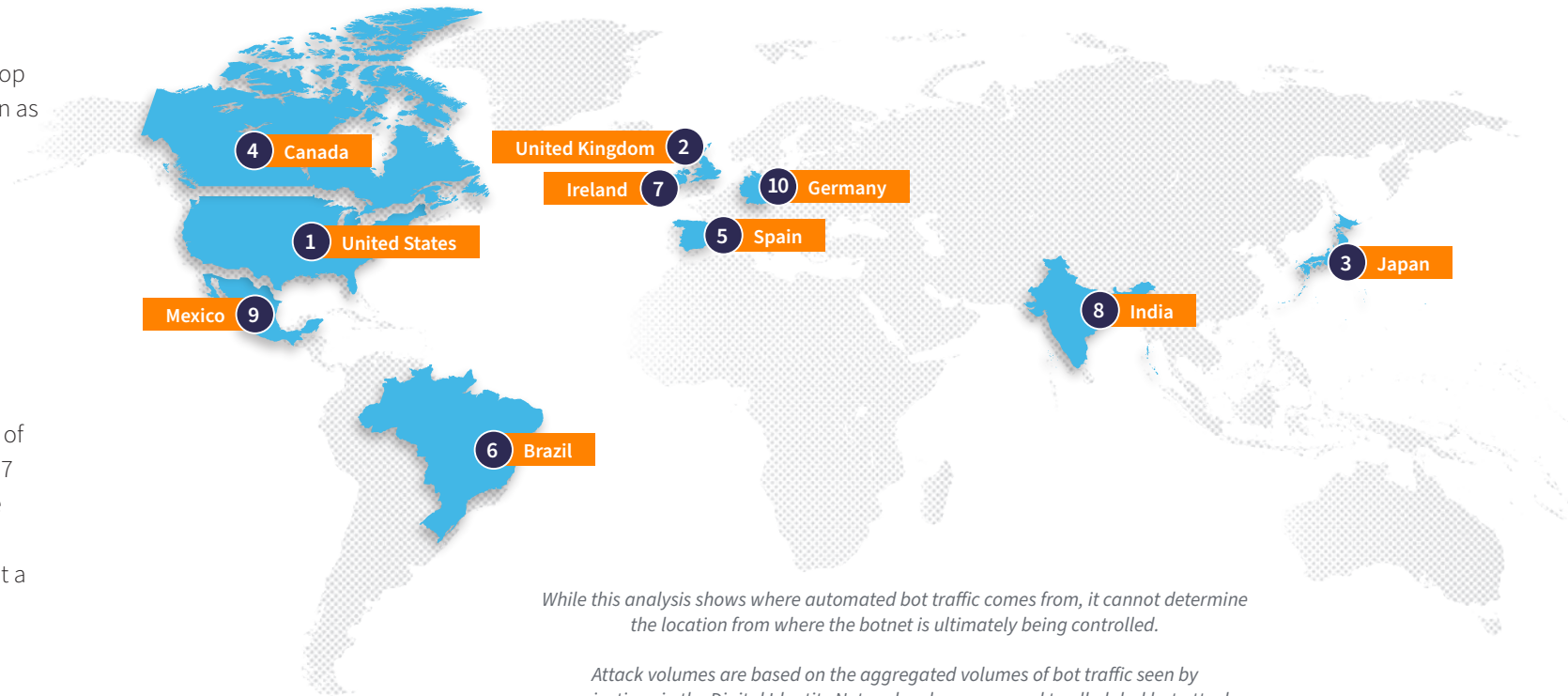
## Spain Contributes Large Growth in Bot Volume to Global Attack Patterns

### Automated Bot Attacks

Brazil and Mexico now both appear on this top ten list, further establishing the LATAM region as a top attack originator.

All regions have recorded a growth in bot volume January-June 2021 in comparison to the same period last year. This was most marked in APAC and LATAM, with EMEA experiencing the smallest growth.

Spain and Mexico replace Australia and the Netherlands on the list of largest originators of bots during this period. Spain has climbed 17 places up the list in comparison to the same period last year, primarily influenced by a large attack testing stolen email addresses at a media streaming site.



*While this analysis shows where automated bot traffic comes from, it cannot determine the location from where the botnet is ultimately being controlled.*

*Attack volumes are based on the aggregated volumes of bot traffic seen by organizations in the Digital Identity Network only, as opposed to all global bot attacks.*

# LARGEST CONTRIBUTORS TO HUMAN-INITIATED CYBERATTACKS, BY VOLUME

## The Philippines Joins List of Top Attackers by Volume Due to Large Attack Targeting Payment Gateway

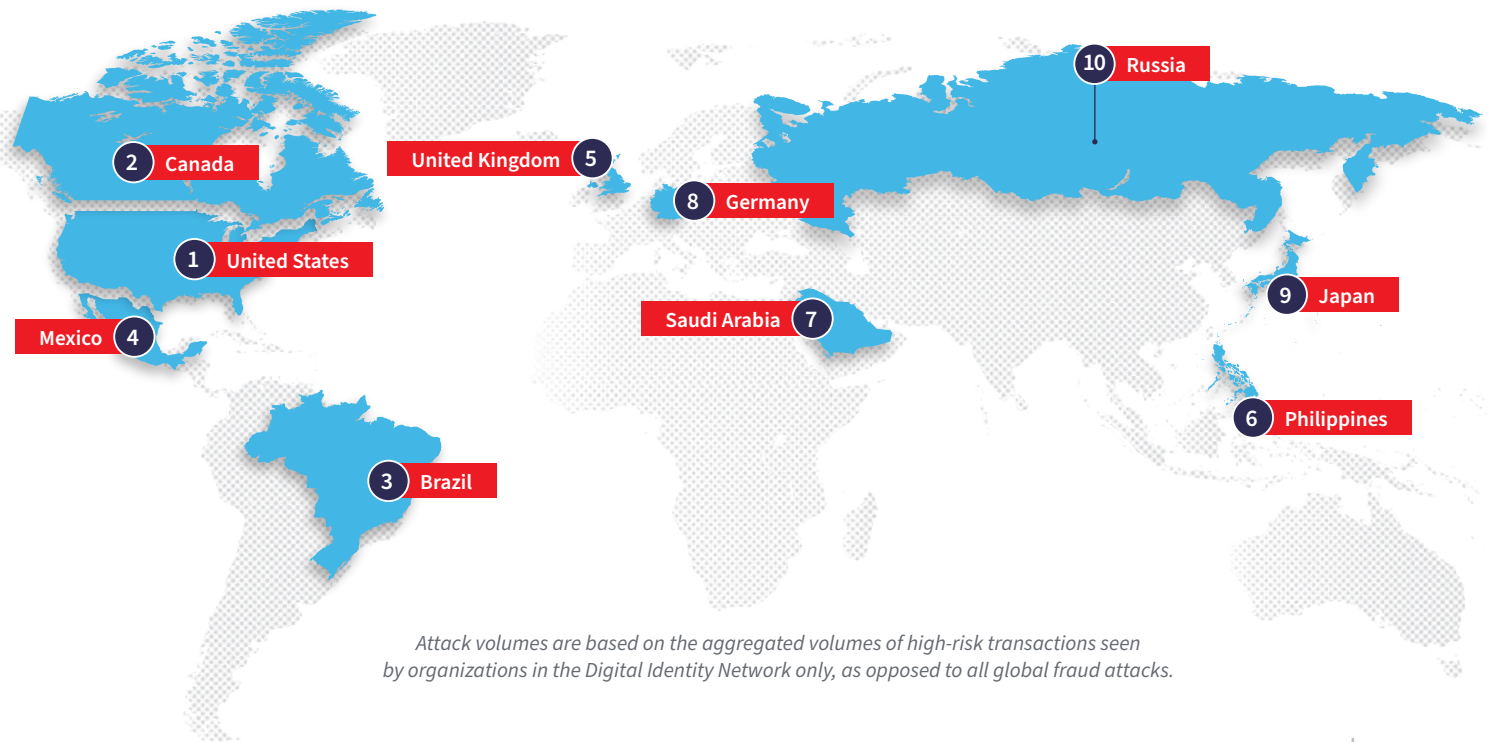
### Human-Initiated Attacks



The U.S., Canada and the UK have been countries where the most consistent attacks have come from. They have been on the top 5 list for the past several years, but continue to be joined by several smaller, growth economies and new regional powerhouses.

Due to the number of attacks from Brazil and Mexico, both remain on the top 5 list of global attackers by country of origin – Mexico appeared on the list for the first time in 2019 as the region established its position on the cybercrime world stage. LATAM continues to generate a high overall volume of fraud attacks.

With attacks from the Philippines and Russia rising, they replace India and the Netherlands on the list of top attackers by volume January-June 2021. The growth in attack volume from the Philippines was largely driven by a credit card testing attack targeting a payment gateway in March.



*Attack volumes are based on the aggregated volumes of high-risk transactions seen by organizations in the Digital Identity Network only, as opposed to all global fraud attacks.*



# 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 in this report includes:

- The key links between 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 reviewed by subsequent organizations before further transactions are processed.



# UNCOVERING NETWORKED ACCOUNT CREATIONS IN GAMING AND GAMBLING REVEALS HIGH-RISK BONUS ABUSE SCENARIOS

## NETWORK IN NUMBERS



**13,000+**

Events linked to confirmed fraud recorded at a source organization.



**At least \$900K**

Fraud blocked.



**95,000+**

Events recorded at other organizations in the Digital Identity Network that were associated with either a device, email address, and / or telephone number that was involved in these original fraudulent events at source organizations.



**At least \$3.2M**

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.



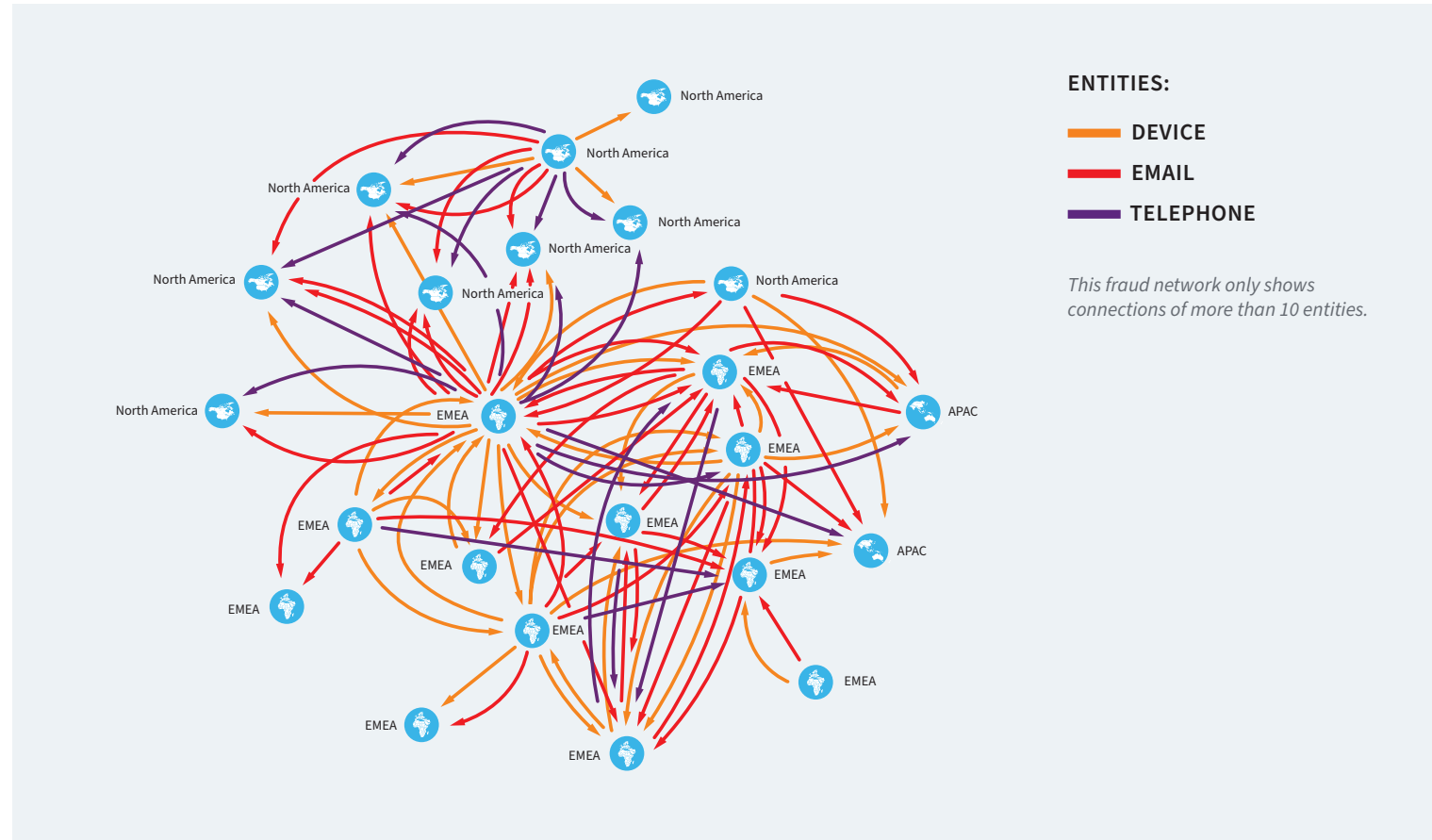
See next page for fraud network visualization

# UNCOVERING NETWORKED ACCOUNT CREATIONS IN GAMING AND GAMBLING REVEALS HIGH-RISK BONUS ABUSE SCENARIOS

This visualization shows a live fraud network targeting the gaming and gambling industry globally. The majority of the transactions within this network are new account creations, (likely trying to exploit new player bonuses) and payments, (likely exiting funds to other accounts). This huge network view of fraud, that crosses over multiple global regions, illustrates just how endemic fraud and money laundering is within the gaming and gambling ecosystem.

Each arrow illustrates entities with confirmed fraud events at an organization in one region, crossing over to another organization in the Digital Identity Network. This fraud network sees a higher proliferation of fraudulent events connected through devices, suggesting multiple different fraud rings.

Detailed analysis shows fraudsters working across regions and evidence of shared stolen identity or payment data.





# LATAM FINANCIAL SERVICES FRAUD NETWORK EXTENDS ITS REACH TO GLOBAL GEOGRAPHIES

## NETWORK IN NUMBERS



**34,000+**

Events linked to confirmed fraud recorded at a source organization.



**101,000+**

Events recorded at other organizations in the Digital Identity Network that were associated with either a device, email address, and / or telephone number that was involved in these original fraudulent events at source organizations.



**Network Fraud**

Fraudulent transactions in this network are a mixture of new account creations, logins and payments.

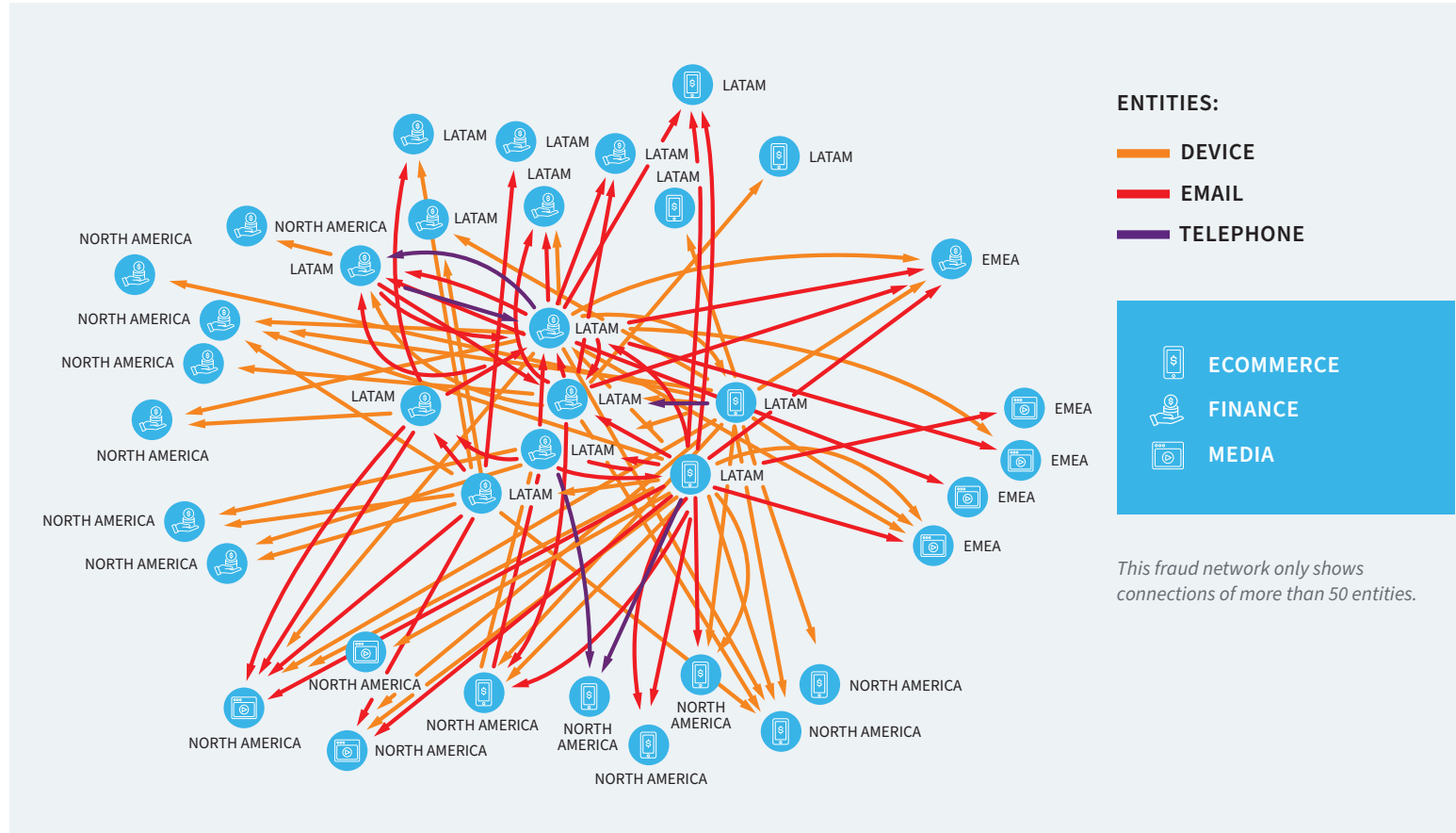


See next page for fraud network visualization

# LATAM FINANCIAL SERVICES FRAUD NETWORK EXTENDS ITS REACH TO GLOBAL GEOGRAPHIES

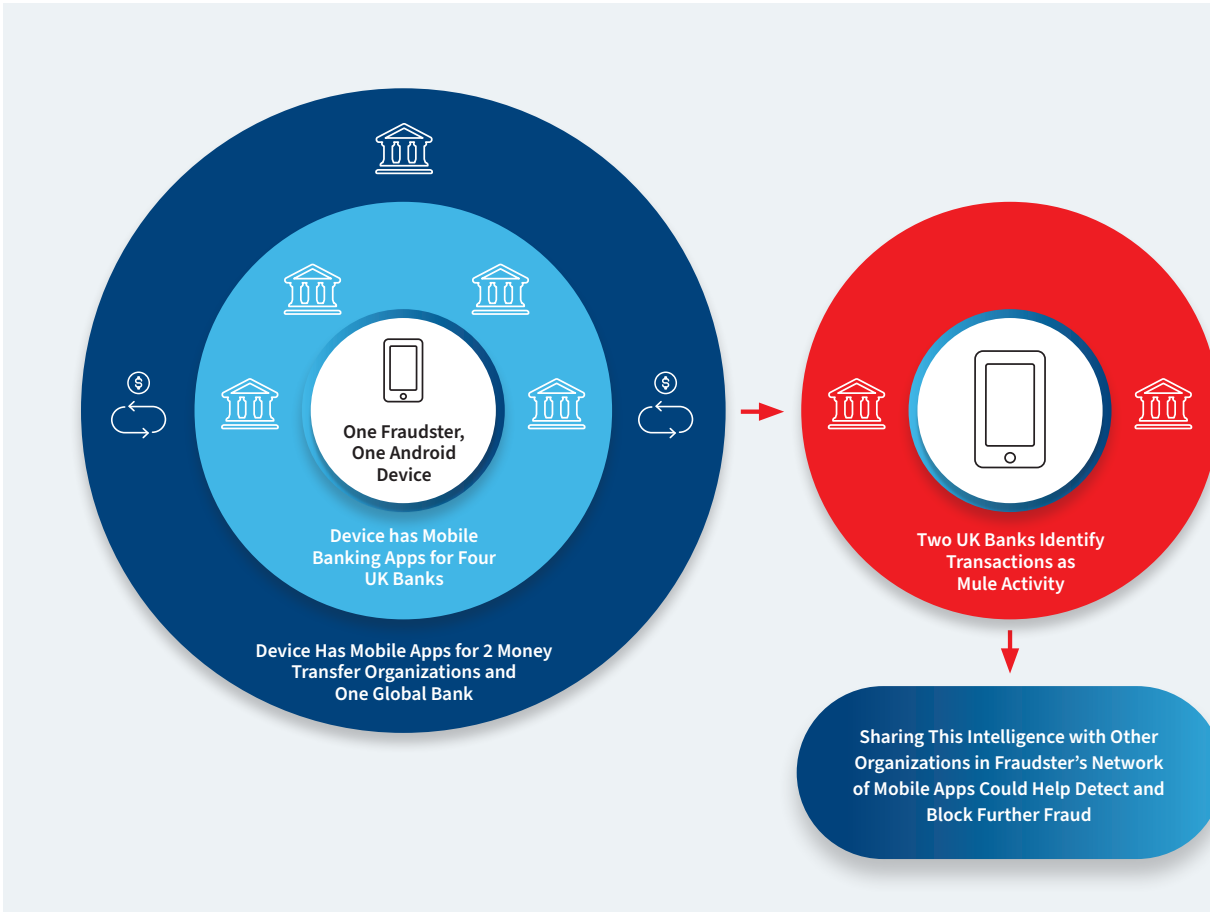
This visualization shows a financial services fraud network originating in LATAM, with connections to several financial services, ecommerce and media organizations in North America, as well as media organizations and a financial services provider in EMEA. This global, distributed pattern of fraudulent behavior indicates how the proceeds of crime committed in LATAM may then be distributed across multinational services worldwide.

As with the previous network, each arrow illustrates entities with confirmed fraud events at an organization in LATAM, crossing over to other organizations globally. This fraud network sees a high proliferation of fraudulent events connected through devices and email addresses, suggesting multiple different fraud rings, as well as possible stolen email address abuse.



# DETECTING NETWORKED FRAUD ON A PER USER SCALE

## Mule Hunting Across Networks of Mobile Apps



While the fraud networks detailed on the previous pages document the links between confirmed fraud events across organizations and regions, the Digital Identity Network can also identify networked fraud on a per user basis, when one fraudster is operating on one device, but targeting multiple organizations via several different apps.

Having the ability to link fraudulent activity across apps within the same device, as well as on high-risk activity across different devices is key to detecting both macro and micro fraud networks.

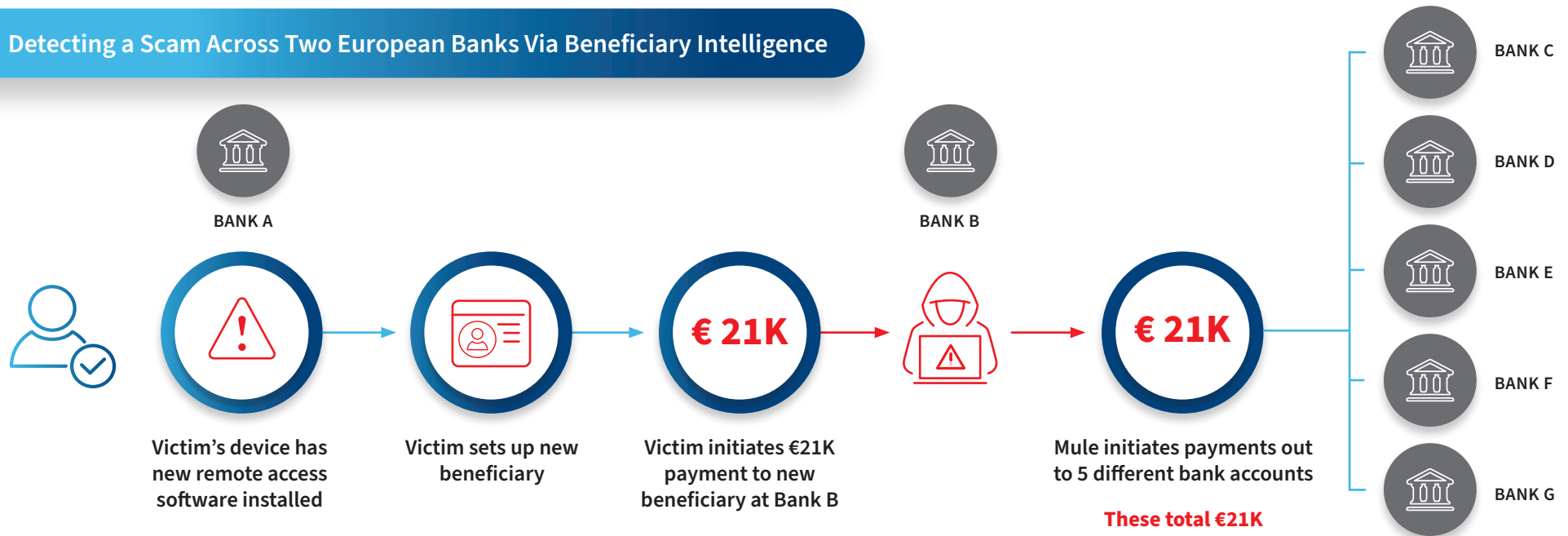
# DETECTING NETWORKED FRAUD ACROSS THE ONLINE BANKING ECOSYSTEM

## Mule Hunting Across Global Payments: Monitoring Transactions from Payer to Beneficiary

Detecting mule networks also relies on the ability to monitor payments from the payer to the beneficiary. This can be particularly challenging when the payment is made by the genuine customer, coerced via a scam or social engineering fraud.

Detecting unusual activity via the beneficiary can help protect good customers making payments to accounts linked to known mule networks.

### Detecting a Scam Across Two European Banks Via Beneficiary Intelligence





JANUARY-JUNE 2021 ANALYSIS: ACROSS THE CUSTOMER JOURNEY

03

JANUARY-JUNE 2021 ANALYSIS:  
**ACROSS THE  
CUSTOMER  
JOURNEY**



# CUSTOMER JOURNEY HIGHLIGHTS: JANUARY-JUNE 2021



## NEW ACCOUNT CREATIONS

Highest attack rate of all use cases.

**1 in every 11** transactions in the Digital Identity Network is an attempted attack.



## LOGINS

**52% growth** YOY in automated bot volume attempting account takeovers.

Higher percentage of attacks via the mobile channel in comparison to last year.



## PAYMENTS

Highest volume of attacks in comparison to all other use cases.

**18% growth** YOY in automated bot volume, likely testing stolen credit card credentials on payment transactions.



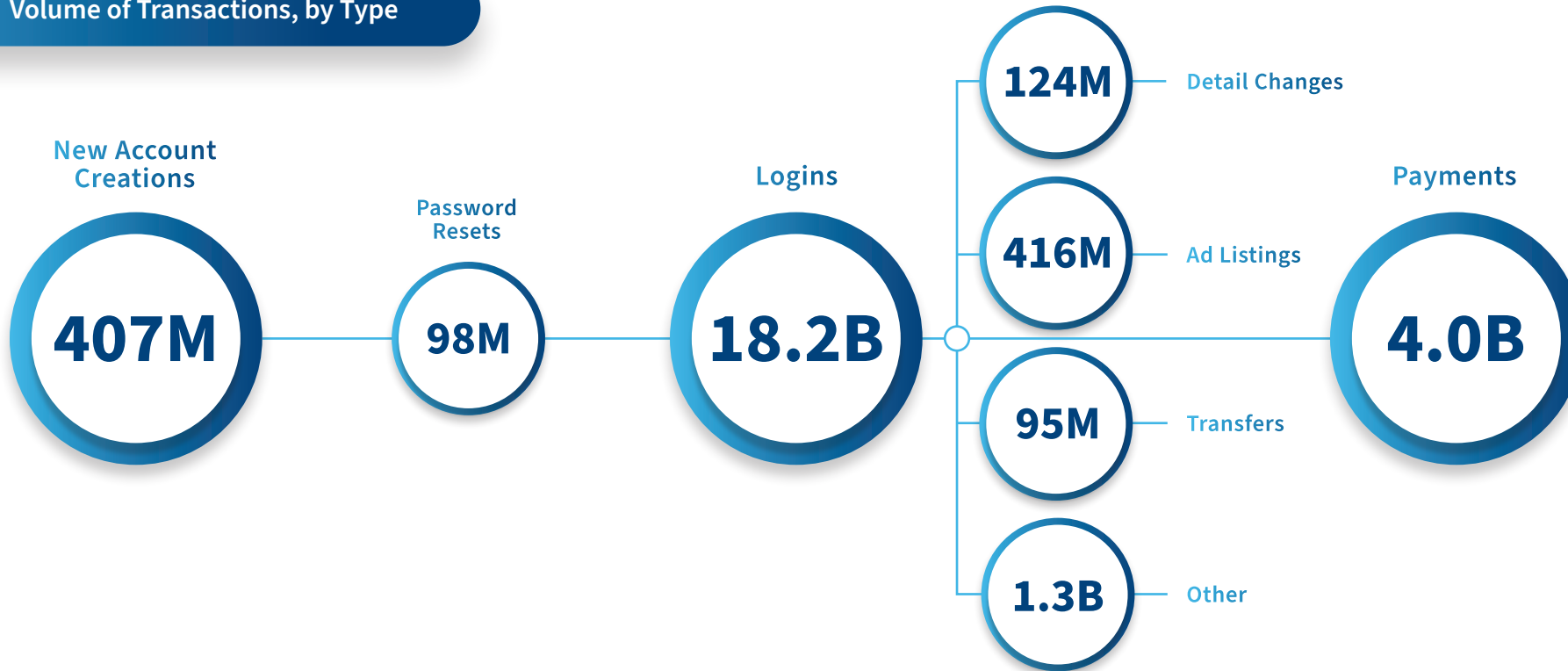
## PASSWORD RESETS

Of the non-core use cases, password resets see the highest rate of attack this period, at **3.8%**.

# VOLUME OF TRANSACTIONS BY USE CASE ACROSS THE ONLINE JOURNEY

Tracking All Customer Touchpoints for Enhanced Risk Decisioning








## Volume of Transactions, by Type





# ATTACK RISKS ACROSS CORE TOUCHPOINTS




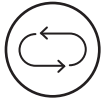





Desktop Transactions See Highest Rate of Attack Across All Core Use Cases

	 <b>NEW ACCOUNT CREATIONS</b>	 <b>LOGINS</b>	 <b>PAYMENTS</b>
<b>RISK TRENDS</b>	<p>Human-initiated attacks have declined across the board for new account creation transactions.</p> <p>However, the automated bot volume targeting these transactions remains strong, rising to a similar level seen at the beginning of 2020.</p> <p>Likewise, the risk for new account creations remains high, with around one in every 11 transactions representing a potential attack.</p>	<p>Login transactions continue to experience low overall attack rates due to a high volume of transactions from trusted and returning customers. However, automated bot attacks attempting account takeovers have grown 52% YOY.</p> <p>Account takeovers are also shifting further towards the mobile channel, with 44% of attacks now targeting mobile, compared to 36% last year.</p>	<p>Payment transactions continue to see the highest volume of attacks across all use cases, with fraudsters cashing out successful fraud attacks via a payment event.</p> <p>Bots targeting payment transactions, likely testing stolen credit card credentials, have also risen by 18% YOY.</p>
<b>ATTACK RATE</b>			
 <b>OVERALL</b>	8.9%	0.4%	2.5%
 <b>DESKTOP</b>	<b>13.2%</b>	<b>0.6%</b>	<b>3.1%</b>
 <b>MOBILE BROWSER</b>	8.3%	0.5%	2.7%
 <b>MOBILE APP</b>	2.6%	0.2%	1.6%



# ATTACK RISKS ACROSS ADDITIONAL HIGH-RISK TOUCHPOINTS

Password Resets and Detail Changes Represent Potential Precursor to Fraud Attacks

	 <b>PASSWORD RESETS</b>	 <b>DETAIL CHANGES</b>	 <b>AD LISTINGS</b>	 <b>TRANSFERS</b>	 <b>OTHER</b>
<b>RISK SUMMARY</b>  Password resets enable fraudsters to take over online accounts, often using stolen credentials. Access to the account then enables future actions, such as payments, to be initiated by the fraudster.  There were two large attacks targeting password resets during this period, likely acting as a precursor to attempted fraud attacks, contributing to a high overall attack rate.	Changes to account details enable fraudsters to amend key account information. Changing a phone number, for example, means that subsequent events, such as SMS one-time passcode (OTP) authentication checks, are sent to the fraudster.  There continues to be an elevated risk of this type of attack via the mobile app.	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.	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.	Encompassing several other high-risk touchpoints such as new channel registrations, standing order mandates, direct debits and beneficiary modifications.	
<b>ATTACK RATE</b>					
 <b>OVERALL</b>	3.8%	1.2%	0.5%	0.9%	1.8%
 <b>DESKTOP</b>	<b>6.8%</b>	0.8%	0.4%	<b>2.6%</b>	2.6%
 <b>MOBILE BROWSER</b>	1.3%	0.8%	<b>1.2%</b>	0.5%	<b>2.8%</b>
 <b>MOBILE APP</b>	0.8%	<b>2.0%</b>	0.4%	0.4%	0.9%

04

JANUARY-JUNE 2021 ANALYSIS:

# REGIONAL TRENDS

34 +7.09%

56 +1.13%

102 +7.51%

397 +2.14%

183 +5.10%

206 +1.17%

992 +6.39%

# REGIONAL HIGHLIGHTS: JANUARY-JUNE 2021



## APAC



**+60%**  
**growth** in transaction  
volume YOY.



**-8%**  
**decline** in human-  
initiated attacks YOY.



**+86%**  
**growth** in bot  
volume YOY.



## EMEA



**+19%**  
**growth** in transaction  
volume YOY.



**-25%**  
**decline** in human-  
initiated attacks YOY.



**+13%**  
**growth** in bot  
volume YOY.



## LATAM



**+57%**  
**growth** in transaction  
volume YOY.



**-1%**  
**decline** in human-  
initiated attacks YOY.



**+84%**  
**growth** in bot  
volume YOY.



## NORTH AMERICA



**+28%**  
**growth** in transaction  
volume YOY.



**-1%**  
**decline** in human-  
initiated attacks YOY.



**+42%**  
**growth** in bot  
volume YOY.

# IDENTITY ABUSE INDEX BY REGION

## LATAM and APAC Continue to Experience Most Volatile Attack Rates, With Significant Daily Peaks Throughout 2021

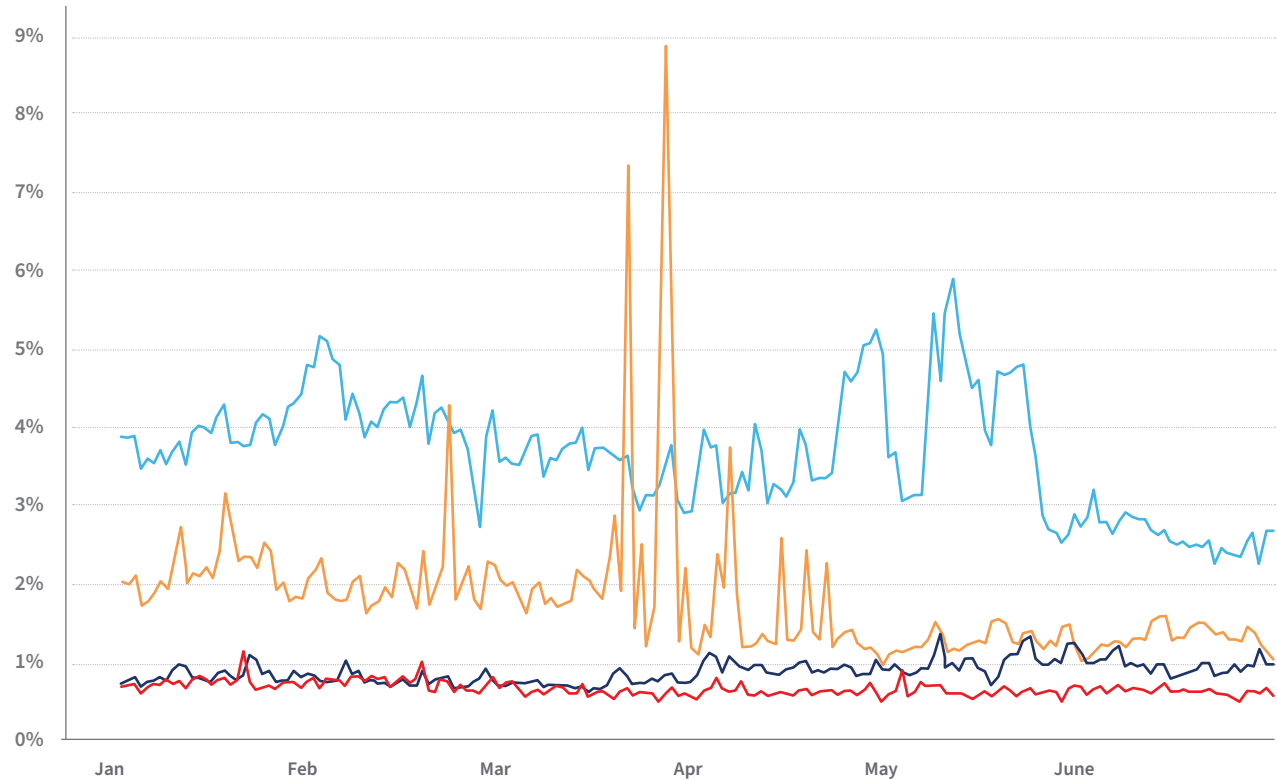
● APAC ● EMEA ● LATAM ● NORTH AMERICA

**LATAM** continues to record the highest daily attack rates of all regions overall, with several attack peaks recorded throughout 2021.

**APAC** records several extremely large bot attack peaks, despite a noticeable downward trend in daily attack rates March-June 2021.

**North America** has recorded increasing daily attack rates March-June 2021, noticeably overtaking the EMEA daily attack rate, a trend that is anomalous with previous periods.

**EMEA** continues to record lower overall attack rates than any other region, with particularly low bot activity during this period.





# APAC SEES LARGEST GROWTH IN AUTOMATED BOT VOLUME OF ALL GLOBAL REGIONS



APAC

## Digital Transactions Continue Upward Trajectory with Strong Shift to Mobile

### Established and Growth Economies Form Melting Pot of Fraudulent Activity

**APAC** is a diverse region which encompasses a number of advanced digital economies such as Australia, Japan, Hong Kong and Singapore, as well as a number of growth regions such as the Philippines, Indonesia, Bangladesh and Sri Lanka. This proliferation of new to digital economies has contributed, in part, to higher fraud rates across the mobile and desktop platforms in comparison to the global trend, with significantly different attack rates seen across different parts of APAC.

The preferred attack vector in the region is automated bots, which are significantly more prevalent than human initiated attacks and contribute to several very large attack peaks across the period, particularly towards the end of March. There is an interesting downward trend in daily attack rates from March to

June, however. This may be due to the fact that new-to-digital activity as a result of the COVID pandemic has stabilized, making differentiating between trusted customers and potential threats clearer.

In line with trends seen in the Digital Identity Network, media reports in the region suggest bot activity targeting ecommerce is rife, with fraudsters attempting to hack in to trusted user accounts to access cards-on-file to make lucrative purchases.

Fraudsters are also taking advantage of the vaccination drive in APAC. There is a surge in COVID vaccine scams, especially out of Australia and India. Scammers use these scams to steal personal information which is then used to commit further fraud, such as creating new accounts with financial institutions.



### ATTACK SPOTLIGHT IN APAC REGION JAN-JUNE 2021

Large session replay attack targeting a payment gateway, testing stolen credit card details, originating in the Philippines.

A significant credit card testing attack targeting a media site with \$1 and \$2 payment tests, predominantly originating from Indonesia.

# APAC TRANSACTION AND ATTACK PATTERNS



## TOP 5 ATTACK ORIGINATIONS

- 1 Philippines
- 2 Japan
- 3 India
- 4 Pakistan
- 5 China



## TOP 5 ATTACK DESTINATIONS

- 1 U.S.
- 2 Japan
- 3 Australia
- 4 U.K.
- 5 Thailand



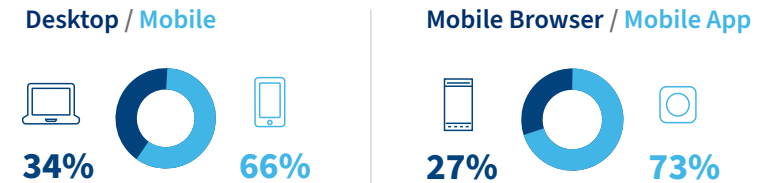
## TRANSACTIONS



### TRANSACTIONS PROCESSED

**2.3B** Growth YOY +60% ▲

### TRANSACTIONS SPLIT BY CHANNEL



## ATTACKS



### AUTOMATED BOT ATTACK VOLUME

Growth YOY +86% ▲

### HUMAN-INITIATED ATTACKS SPLIT BY CHANNEL



### HUMAN-INITIATED ATTACK VOLUME

Decline YOY -8% ▼

# APAC POSITION AGAINST GLOBAL FIGURES

## APAC Continues to See Higher Overall Attack Rates Across All Channels in Comparison to Global Figures

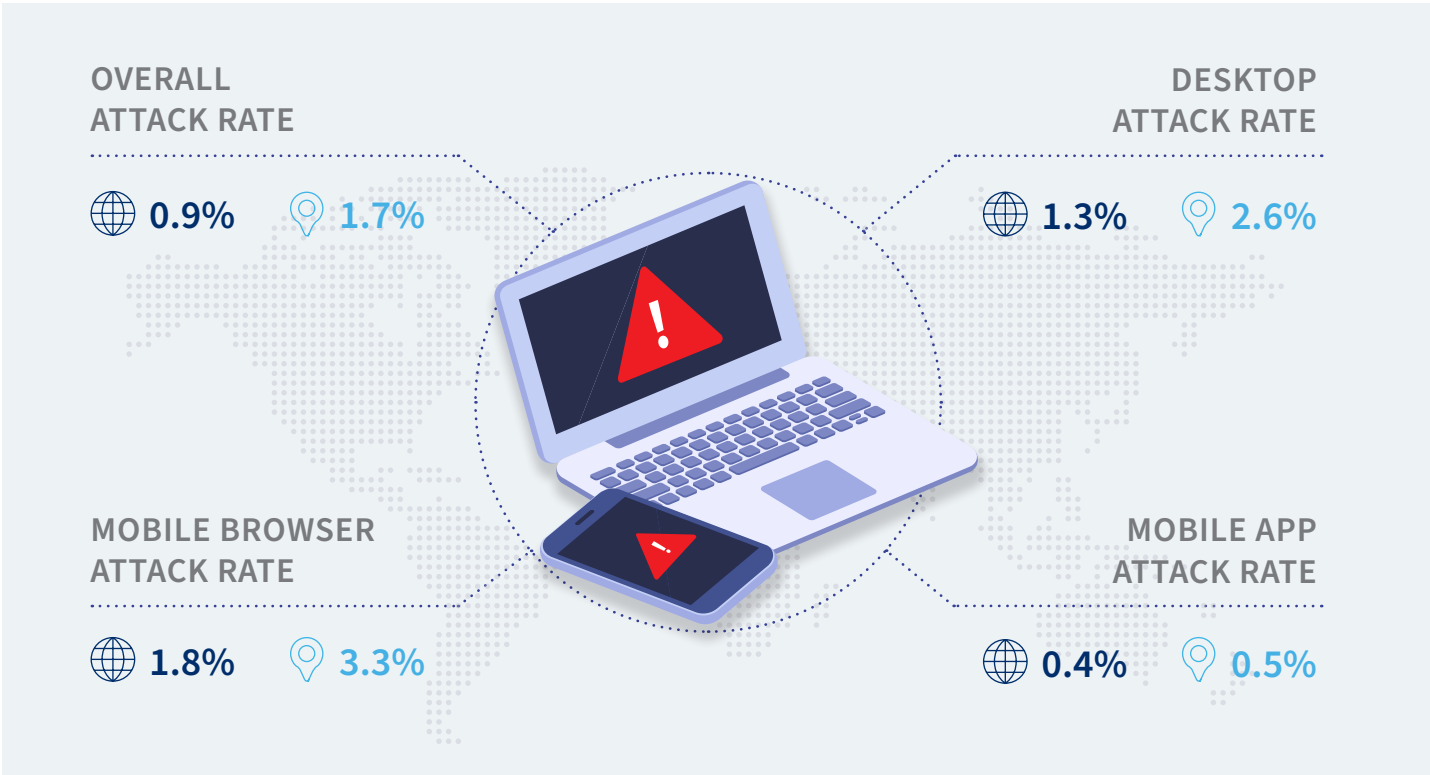


 **GLOBAL**     **APAC**

Attack rates in APAC remain higher than the global averages, although they continue to fall across all channels YOY.

However, the APAC region experienced the strongest growth in automated bot volume of all global regions.

This is reflected in the fact that APAC remains a large contributor to global bot attacks, with Japan and India both appearing on the list of top attack originators globally.



# EMEA SEES LOWEST OVERALL ATTACK RATES WITH SMALLEST GROWTH IN AUTOMATED BOT VOLUME



EMEA

## Mature Digital Markets Drive High Volumes of Trusted Customer Interactions

### High Mobile Transaction Penetration is Pushing Fraud Further Towards Mobile Channel

**EMEA** encapsulates a relatively mature digital environment albeit encompassing some emerging markets such as Eastern Europe and part of Africa. This leads to a relatively stable attack profile with low and declining overall fraud rates recorded in the Digital Identify Network. Given that mature online banking solutions are doing a good job at driving down fraud rates, fraudsters are turning their attention to alternative attack typologies such as COVID-related, romance and investment scams.

The prevalence of scams in Middle Eastern and African markets has been widely reported recently, where digital maturity is lower on the adoption curve. These scams often originate from social media websites with the aim to steal key personal information of victims. This information can then be used to either social engineer the victim to make an authorized payment, create a

synthetic identity or perform an account takeover. Having said this, many more mature digital markets, such as the UK, are also reporting a huge rise in scam attacks in recent months.

The evolution of European regulations and uptake of Strong Customer Authentication (SCA) is starting to have an impact on fraud rates in the ecommerce world with more merchants and issuers adopting 3DS2.x and other strong authentication strategies. However, traditional two-factor authentication methods such as One Time Passcodes (OTP) and Passwords can lead to friction in the payment process, causing a decrease in conversions in some countries where SCA is mandated. To continue to keep fraud low and to provide less friction, merchants and issuers are looking at alternative low friction authentication solutions to minimize friction during the checkout process.



### ATTACK SPOTLIGHT IN EMEA REGION JAN-JUNE 2021

Series of automated bot attacks targeting the ecommerce industry, particularly marketplaces and airlines. These attacks are targeting change of details pages in the customer journey in order to gain access to good customer accounts. They originate mostly from Israel, Germany and the UK.

A large bot attack attempted fraudulent payments at an online marketplace and payment gateway originating in the UAE.



# EMEA TRANSACTION AND ATTACK PATTERNS



## TOP 5 ATTACK ORIGINATIONS

- 1 U.K.
- 2 Saudi Arabia
- 3 Germany
- 4 Russia
- 5 France

## TOP 5 ATTACK DESTINATIONS

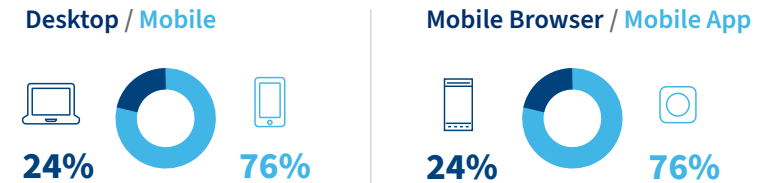
- 1 U.S.
- 2 U.K.
- 3 Russia
- 4 France
- 5 Canada

## TRANSACTIONS



**TRANSACTIONS PROCESSED**  
**9.4B** Growth YOY **+19% ▲**

## TRANSACTIONS SPLIT BY CHANNEL

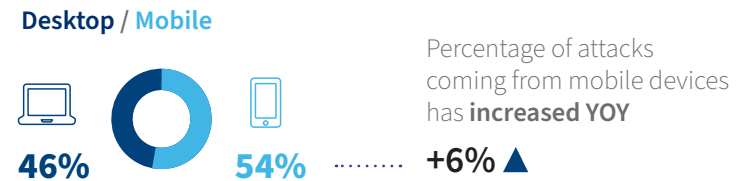


## ATTACKS



**AUTOMATED BOT ATTACK VOLUME**  
 Growth YOY **+13% ▲**

## HUMAN-INITIATED ATTACKS SPLIT BY CHANNEL



**HUMAN-INITIATED ATTACK VOLUME**  
 Decline YOY **-25% ▼**

# EMEA POSITION AGAINST GLOBAL FIGURES

## Low Overall Attack Rates Prevail, With Small Growth in Percentage of Mobile Attacks

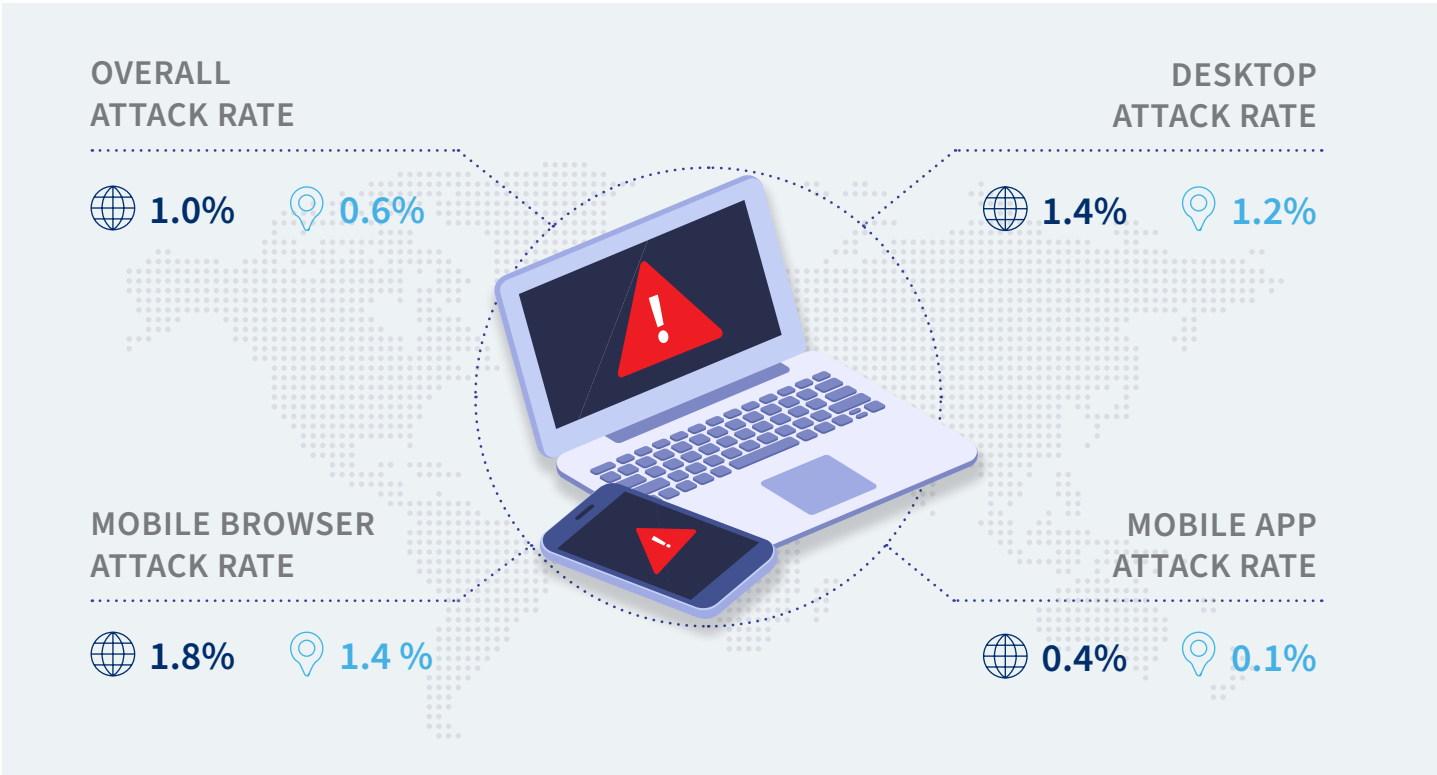


EMEA continues to experience low overall attack rates in comparison to the global averages, driven by a mature digital environment and high volume of trusted mobile app transactions.

The region experienced the biggest decline in the human-initiated attack volume in comparison to other regions.

EMEA also experienced the smallest growth in automated bot volume in comparison to other global regions.

However, the region has recorded a 6% growth in the percentage of attacks coming from mobile devices during this period.



# LATAM SEES HIGHEST INCREASE IN PERCENTAGE OF MOBILE ATTACKS IN COMPARISON TO OTHER REGIONS



LATAM

## Digitalization and Infrastructure Modernization Leads to an Increase in Mobile Transactions

### Cheaper and Easier Digital Banking and Payment Solutions are Shifting the Latin American Banking Paradigm

**LATAM** continues to ride the wave of digital transformation with the rapid growth of digital platforms, online banking, diverse payment methods and ecommerce offerings. While many economies in the region are highly digital, large swathes of the population still predominantly access online services via a mobile device only. This means that digital-only and virtual banks can help facilitate financial inclusion for the unbanked and underbanked via mobile banking provision.

This rapid digitalization and infrastructure modernization contributes to the fact that LATAM continues to see the highest daily attack volumes globally, with a strong emphasis on automated bot attack growth. For the first half of the year, it also saw three distinct peaks in attack rates in January, April and May.

In addition, to support COVID recovery, the South American governments released stimulus packages which led to large numbers of people opening digital bank accounts for the first time. While this led to a growth in online banking transactions, it also exposed a huge population of new-to-digital consumers to fraud and potential scams.

For many of these new digital banking and payment organizations, simple digital onboarding facilitated a rapid influx of new customers. However, these same simple onboarding processes are often heavily targeted by fraudsters, particularly in countries where KYC checks are in their infancy and there is no national standard of identity documentation. A big facilitator of this type of fraud is the victim's mobile phone handset. The region is seeing high volumes of handset theft that fraudsters are then using to intercept online banking credentials.



### ATTACK SPOTLIGHT IN LATAM REGION JAN-JUNE 2021

Large bot attack attempting new account creations at financial institutions coming from Mexico.

Automated bot attacks also attempted account takeovers targeting media streaming organizations. These predominantly came from Brazil, Argentina and Colombia and were testing stolen email addresses.

# LATAM TRANSACTION AND ATTACK PATTERNS



## TOP 5 ATTACK ORIGINATIONS

- 1 Brazil
- 2 Mexico
- 3 Colombia
- 4 Peru
- 5 Argentina

## TOP 5 ATTACK DESTINATIONS

- 1 Brazil
- 2 U.S.
- 3 Chile
- 4 U.K.
- 5 Mexico

## TRANSACTIONS



### TRANSACTIONS PROCESSED

**1.2B** Growth YOY **+57% ▲**

### TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



## ATTACKS

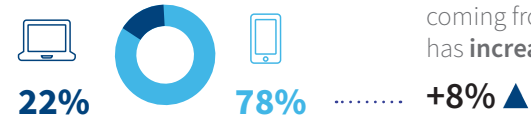


### AUTOMATED BOT ATTACK VOLUME

Growth YOY **+84% ▲**

### HUMAN-INITIATED ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



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

**+8% ▲**



### HUMAN-INITIATED ATTACK VOLUME

Decline YOY **-1% ▼**



# LATAM POSITION AGAINST GLOBAL FIGURES

## Small Decline in Human-Initiated Attacks Coupled With Strong Bot Growth



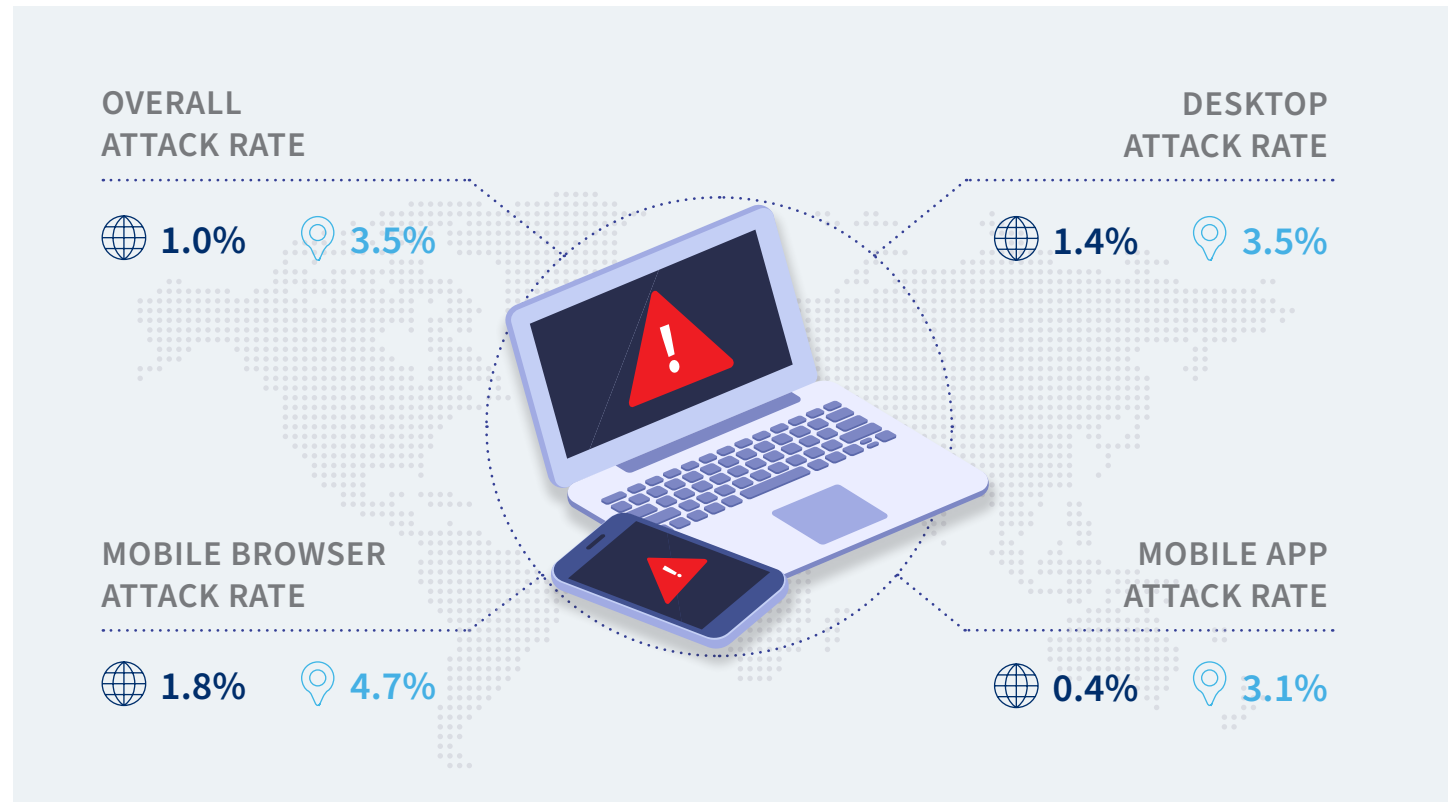
 GLOBAL  LATAM

Attack rates in LATAM remain the highest of all global regions, across all use cases.

Rapid digital transformation is driving a volatile attack environment where bot attack volumes are on an upward trajectory and daily attack rates show several strong peaks across the period.

The mobile channel is particularly susceptible to attacks in the region, with high attack rates across both mobile browser and mobile app transactions. All other global regions record much lower attack rates on mobile app transactions.

This is likely driven by the fact that mobile is facilitating financial inclusion and is therefore targeted more heavily than desktop for some use cases. The percentage of attacks targeting the mobile channel has increased 8% YOY.



# NORTH AMERICA'S ESTABLISHED ECONOMIES CONTINUE STRONG FIGHT AGAINST FRAUD

## North America's Fight Against BOT Attacks Continues, With Some Indication that Fraud Risk in the Region is Growing



### Large Growth in Automated Bot Volume Contributes to More Volatile Daily Attack Pattern

**North America** typically sees low attack rates on a par with its European counterparts due to its mature and well-established digital economy. However, this period has recorded a slightly more volatile attack trend for the region. There was a notable uptick in daily attack rates during the second quarter, perhaps fueled by the further loosening of COVID restrictions for many states across the U.S. and Canada, with fraudsters hoping to capitalize on the more diverse consumer travel and spending footprint.

COVID scams continue to be an issue in the United States as well, where government stimulus packages

have created many opportunities for fraud to flourish. Fraudsters are pretending to be from legitimate government or bank departments, and are asking for victims to verify personal information or provide a small processing fee so that they can send “the stimulus check” faster.

Fraudsters have also continued to use identity spoofing techniques to make multiple fraudulent claims to register phony businesses and receive further government support.



### ATTACK SPOTLIGHT IN NORTH AMERICAN REGION JAN-JUNE 2021

Large bot attack attempting to register new social media accounts en masse. These bots are using computer-generated email addresses to register fake accounts, presumably to use in scams, for fake news or spamming attacks.

Large bot attack targeting several ecommerce giants, attempting new account creations to take advantage of new customer bonuses.

# NORTH AMERICA TRANSACTION AND ATTACK PATTERNS



## TOP ATTACK ORIGINATIONS



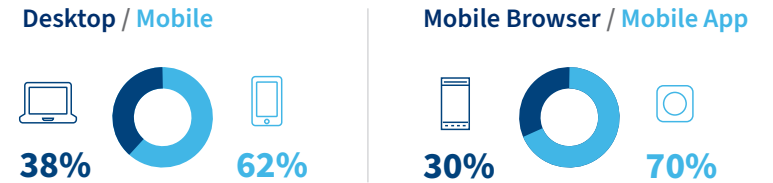
## TOP 5 ATTACK DESTINATIONS



## TRANSACTIONS



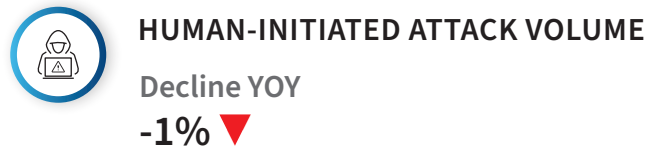
## TRANSACTIONS SPLIT BY CHANNEL



## ATTACKS



## HUMAN-INITIATED ATTACKS SPLIT BY CHANNEL



# NORTH AMERICA POSITION AGAINST GLOBAL FIGURES



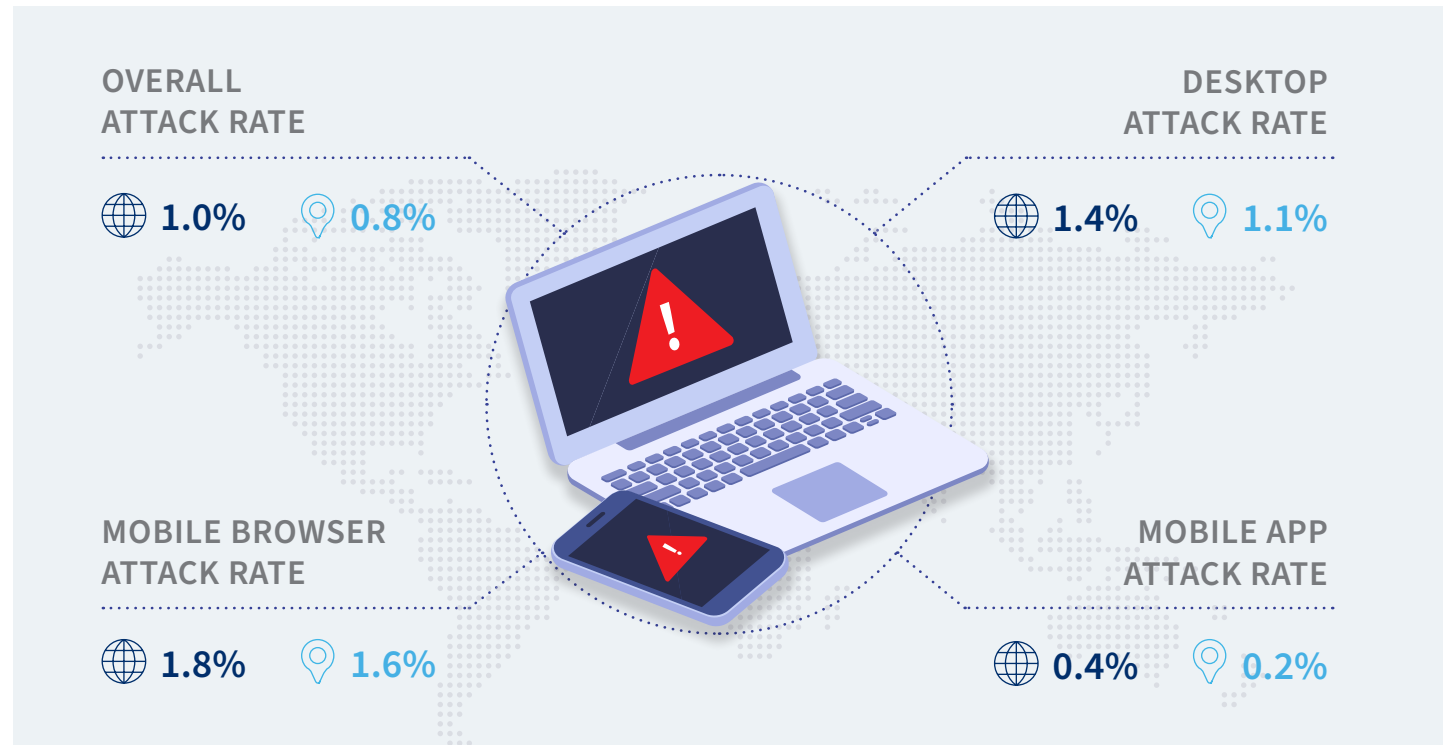
## Growth in Attack Rate March Through June Indicates Heightened Risk Environment

GLOBAL NORTH AMERICA

North America continues to experience low overall attack rates in comparison to the global averages.

There is some indication of a growing risk environment in North America, however: there was a smaller decline in human-initiated attacks this period, coupled with a large increase in automated bot volume.

In addition, the daily attack rate as shown on the regional Identity Abuse Index overtook that of EMEA from mid-March through to the end June 2021.





JANUARY-JUNE 2021 ANALYSIS: INDUSTRY OPPORTUNITIES

05

JANUARY-JUNE 2021 ANALYSIS:

# INDUSTRY OPPORTUNITIES



# INDUSTRY HIGHLIGHTS: JANUARY-JUNE 2021



## FINANCIAL SERVICES

Low overall attack rates, driven by a high volume of repeat login transactions from trusted customers.

The exception is for payment transactions, which continue to be attacked at a higher rate than any other industry, presenting a key opportunity for fraudsters to cash out.



## ECOMMERCE

Ecommerce merchants in the Digital Identity Network continue to experience low overall attack rates.

There was also a slight decline in automated bot activity YOY.










## MEDIA

New account creations attacked at a higher rate than any other industry, with fraudsters using media organizations to test stolen identity data.

Large increase in automated bot activity targeting media organizations.








# INDUSTRY OVERVIEW: TRENDS AND ATTACK PATTERNS

Media Organizations Continue to Bear the Brunt of Identity Testing Attacks

INDUSTRY OVERVIEW	 ALL INDUSTRY SUMMARY	 FINANCIAL SERVICES	 ECOMMERCE	 MEDIA
RISK TRENDS	Desktop transactions continue to be attacked at the highest rate of all channels.	Despite high attack volumes, overall attack rates are extremely low, driven by large volumes of repeat, trusted transactions.  The exception is on payments transactions, which are attacked at a higher rate than other industries	Attack rates in ecommerce remain relatively low and continue to decline.  A modest decline in automated bot volume.	New account creations and logins attacked at a higher rate than any other industry.  Large growth in automated bot volume targeting social media platforms, media streaming sites and gaming and gambling operators.
ATTACK RATE				
 OVERALL	1.0%	0.7%	1.3%	3.7%
 DESKTOP	<b>1.4%</b>	<b>1.0%</b>	<b>1.8%</b>	<b>3.7%</b>
 MOBILE	0.8%	0.6%	1.0%	3.6%

# FINANCIAL SERVICES: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Financial Services Payment Transactions Continue to Record Highest Attack Rate of All Industries

<b>FINANCIAL SERVICES OVERVIEW</b>	 <b>NEW ACCOUNT CREATIONS</b>	 <b>LOGINS</b>	 <b>PAYMENTS</b>
<b>RISK TRENDS</b>	<p>Significant drop in attack volume / mobile app attack rate due to large bot attack targeting mobile app new account creations in January 2020 which led to a huge peak in attacks during this period.</p> <p>However, growth in attack rates across desktop and mobile browser transactions.</p>	<p>The overall attack rate on login transactions remains low due to a high volume of regular transactions from trusted customers.</p> <p>It remains significantly safer to login to a financial services account from a mobile app than a desktop.</p>	<p>Although financial services payments transactions see a higher rate of attack than other industries, attack rates continue to decline across the board.</p> <p>Desktop and mobile browser transactions are targeted at a significantly higher rate than mobile app transactions, with fraudulent payment representing significant opportunity for fraudsters to cash out or move money across mule accounts in the financial services ecosystem.</p>
<b>ATTACK RATE</b>			
 <b>OVERALL</b>	<p>6.2%</p>	<p>0.3%</p>	<p>2.9%</p>
 <b>DESKTOP</b>	<p><b>11.6%</b></p>	<p><b>0.5%</b></p>	<p><b>3.6%</b></p>
 <b>MOBILE BROWSER</b>	<p>4.4%</p>	<p>0.4%</p>	<p>3.5%</p>
 <b>MOBILE APP</b>	<p>2.0%</p>	<p>0.1%</p>	<p>1.3%</p>



# THE RISE OF VIRTUAL BANKS

## Analyzing Changing Consumer Behavior Across Traditional and Virtual Banks

Virtual banks offer all products and services online and have no branch network.

They are sometimes sub-brands of traditional banks, but often operate completely independently from the traditional banking model.

They are increasingly helping to facilitate financial inclusion for unbanked and underbanked populations within growth economies as many prioritize mobile apps over browser transactions.

### GROWTH IN TRANSACTION VOLUME YOY



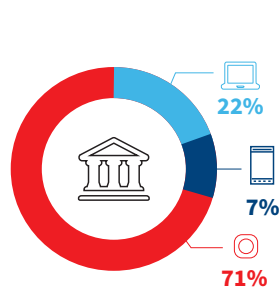
**37%**  
Traditional Banks



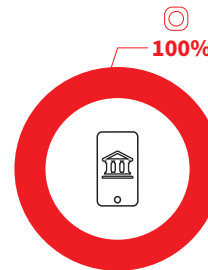
**68%**  
Virtual Banks

### CHANNEL PREFERENCE

● MOBILE APP ● DESKTOP ● MOBILE BROWSER



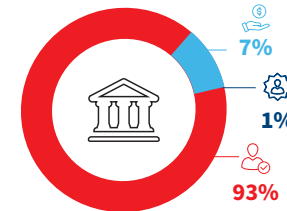
**Traditional Banks**  
Mixture of desktop and mobile transactions



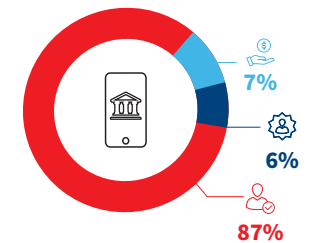
**Virtual Banks**  
All mobile app transactions

### TRANSACTION PROFILE

● ACCOUNT LOGINS ● PAYMENTS ● NEW ACCOUNT CREATIONS



**Traditional Banks**  
Low percentage of new account creations



**Virtual Banks**  
Higher proportion of new account creations as consumers move towards digital-only model

# ATTACK SPOTLIGHT: IDENTIFYING FRAUD TARGETING CRYPTOCURRENCY WALLETS

The Digital Identity Network records many examples of confirmed fraud events between cryptocurrency wallets and financial services organizations.

These are likely to be predominantly account takeover transactions and payment events where fraudsters are either moving money between mule accounts to cryptocurrency wallets, or taking over good customer accounts and siphoning money off to cryptocurrency accounts.

The Digital Identity Network has also seen several examples of sophisticated cryptocurrency scams, with the following attack typology:



## THE SCAM INTRODUCTION

A customer responds to a cryptocurrency investment phishing or smishing message. The fraudster then typically makes contact with the customer, socially engineering them into believing they are investing in a legitimate cryptocurrency platform. This may be supported by a fake app or website.



## METHODOLOGY

The good customer sets up a cryptocurrency account with a legitimate wallet provider, believing that they are making a transfer to that provider.










## ATTACK

The fraudster then tricks the customer into transferring the balance to a different account, usually in a foreign country, presumably under the premise that the account details for the legitimate cryptocurrency wallet are incorrect. The payment is initiated by the legitimate account holder and therefore bypasses many fraud and security checks. It is rarely recovered.

# ECOMMERCE: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Attack Rates Continue to Decline as Merchants Shore Up Fraud Controls

<p>ECOMMERCE OVERVIEW</p>	 <p>NEW ACCOUNT CREATIONS</p>	 <p>LOGINS</p>	 <p>PAYMENTS</p>
<p>RISK TRENDS</p>	<p>New account creations from a desktop continue to be attacked at a higher rate than any other use case, with more than one in every 10 transactions identified as a potential attack.</p> <p>While the overall attack rate remains low, there was a significant increase in bots targeting new account creations YOY.</p>	<p>Although ecommerce merchants experience a higher rate of account takeover attempts in comparison to financial services, overall attack rates remain relatively low, and continue to decline across all channels YOY.</p>	<p>Payment transactions in the ecommerce customer journey represent an opportunity for fraudsters to monetize stolen credentials.</p> <p>Overall attack rates are declining however, indicating that merchants are deploying robust authentication and authorization strategies to assess the risk of a payment transaction.</p>
<p>ATTACK RATE</p>			
 OVERALL	5.9%	0.9%	2.1%
 DESKTOP	<b>11.8%</b>	1.2%	<b>2.8%</b>
 MOBILE BROWSER	3.5%	<b>6.0%</b>	1.3%
 MOBILE APP	1.2%	0.4%	2.0%

# BUY NOW PAY LATER BOOMS THROUGH COVID-19

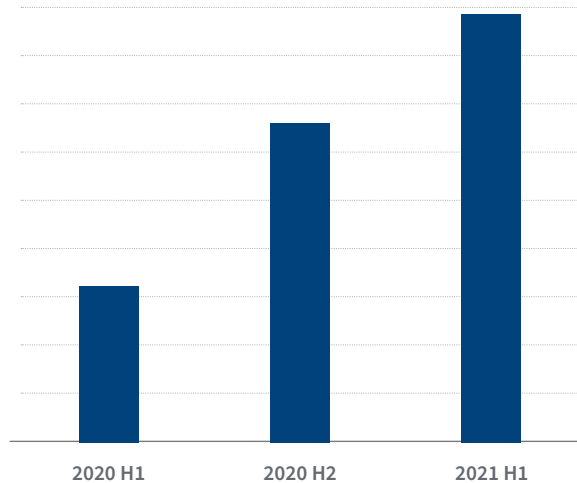
## Mobile Devices Drive High Take-Up for Post-Payments Market

The buy now pay later (BNPL) market has boomed over the last 12 months, offering consumers the flexibility to delay payments, as well as split them across a flexible installment plan.

This market presents potential risk to providers, however, with fraudsters looking for ways to exploit the fact they can walk away with goods at either a fraction of the retail price, or even zero cost.

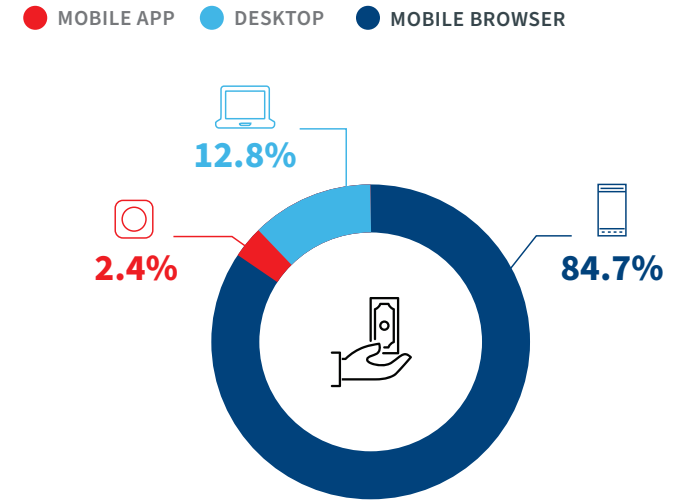
This makes reliable and robust risk assessment, throughout the online customer journey, more critical than ever.

### TRANSACTION GROWTH



BNPL transactions have grown 182% YOY in the Digital Identity Network, reflecting the fact that COVID-19 is changing the way consumers pay for goods and services online.

### TRANSACTIONS BY CHANNEL



BNPL transactions are predominantly seen on mobile browsers. This perhaps points to the fact that they help facilitate more spontaneous purchases while consumers are browsing online.



# SECURING ECOMMERCE PAYMENTS WITH 3DS 2.X

## Evolving Regulatory Environment Increases Use of 3DS to Streamline Customer Experience, Corresponding With Declining Attack Rates Across Ecommerce Payments

The 3DS protocol provides a secure framework to link the acquirer with the issuer in order to authenticate a cardholder during an ecommerce transaction. It was updated in 2018 to include a mobile component and to further streamline the customer experience without compromising security.

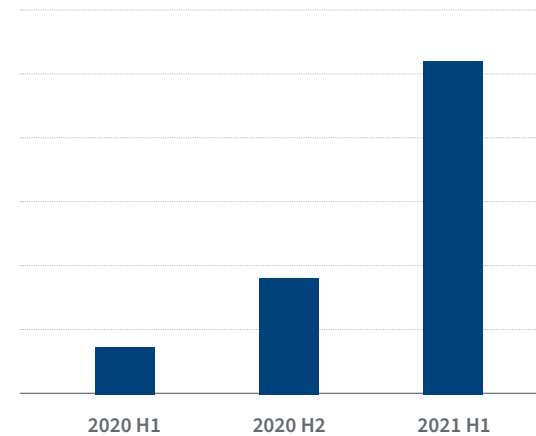
The ability to attach historical context to a cardholder's device, location, email address and online behavior, even when they are interacting with 3DS 2.x for the first time, is critical for success.

Understanding trust and risk across the online customer journey can also help reduce friction for legitimate customers, while detecting fraud in near real time.

The Digital Identity Network can help merchants, acquirers and issuers share intelligence related to online consumers, identifying both trust and risk across organizations, industries and regions.

- **The Digital Identity Network has recorded a significant growth in 3DS transactions YOY.**
- **This growth in 3DS transactions also corresponds with a declining attack rate across ecommerce payments YOY, suggesting that the protocol is succeeding in reducing fraud.**








### 3DS TRANSACTIONS



- **The Digital Identity Network has recorded a 623% growth in 3DS transactions YOY.**
- **Ecommerce payments attack rate has declined 36% YOY.**

# MEDIA: OVERVIEW OF TRENDS AND ATTACK PATTERNS

## Media Organizations Hit by Wave of Automated Bot Attacks Testing Stolen Credentials








MEDIA OVERVIEW	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
<b>RISK TRENDS</b>	<p>While attack rates on new account creations have declined, they remain higher for media organizations than any other industry.</p> <p>It's likely that many of these new account creation attempts comes from fraudsters testing stolen identity data on companies which typically have lower barriers to entry.</p> <p>Attempts are made to abuse new customer bonuses, or to resell trial periods for financial gain.</p>	<p>The overall login attack rate is slightly higher for media organizations than other industries, although the attack rate here is also declining.</p> <p>The attack rate on mobile apps remains high, however, and represents a key risk point for media account takeovers.</p> <p>The majority of media bot volume targets login transactions, testing stolen credentials.</p>	<p>Attack rates on media payments are lower than in other industries, likely because they represent less opportunity to “cash out” in comparison to an ecommerce or financial services payment.</p>
<b>ATTACK RATE</b>			
 <b>OVERALL</b>	12.6%	1.1%	1.9%
 <b>DESKTOP</b>	<b>16.2%</b>	0.6%	<b>2.2%</b>
 <b>MOBILE BROWSER</b>	12.1%	0.5%	2.0%
 <b>MOBILE APP</b>	6.3%	<b>5.4%</b>	1.3%

# GAMING AND GAMBLING: OVERVIEW OF TRENDS AND ATTACK PATTERNS

## New Player Bonus Abuse Prompts High Attack Rates at New Account Creations

The new account creation attack rate for gaming and gambling operators is comparable to that seen by media organizations, indicating the huge risk posed at the point of onboarding a new customer.

These operators are particularly attractive to fraudsters as they offer the opportunity to make money via mass sign-up to new player bonuses, and well as representing a potential safe-haven for money laundered across the global financial ecosystem.

ATTACK RATE	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
 OVERALL	9.0%	0.6%	0.9%
 DESKTOP	<b>13.4%</b>	0.4%	0.7%
 MOBILE BROWSER	8.4%	0.3%	0.9%
 MOBILE APP	2.9%	<b>1.7%</b>	<b>1.0%</b>

# TELCO: OVERVIEW OF TRENDS AND ATTACK PATTERNS

## Telco Operators Become Both the Facilitator and the Solution to SIM Swap Fraud

Telco companies represent a unique bridge between both an ecommerce and telecommunications provider, as well as a facilitator for the provision of intelligence and infrastructure to many other industries to support the products and services they offer.

It is for this reason, however that they often become a key target for fraudsters. Not only do they offer the opportunity to steal high-value hardware, they also represent the first stage in the chain of SIM swap fraud, a dangerous precursor to either an SMS OTP interception

(perhaps to facilitate a mobile banking app registration), or an account takeover.








In addition, many telcos are now defined as quad providers, offering fixed, mobile, broadband and media services. This makes them susceptible to the same fraud challenges that a media provider has.

Telcos therefore become an extremely rich target for fraud, as they provide opportunity for fraudsters to set up fake accounts, test stolen credentials, compromise customer

accounts, access high value hardware and control a user’s identity data. This makes protection at every stage of the customer lifecycle absolutely critical, from the point at which a consumer registered for a pre or post-paid account, and then throughout that lifecycle management both online, offline and via the call center.

### Additional Fraud Typologies in Telco include:

- Registration for a post-paid account. For many organizations, if you apply for one phone successfully, you are then pre-approved for an additional number of lines. Additional handsets can be ordered for these additional lines. If the first account is fraudulent this exposes the organization to increased risk.
- Account takeover and handset fraud on upgrades.
- SIM swap fraud in order to use the SIM to call premium rate numbers that the fraudster owns.

	 NEW ACCOUNT CREATIONS	 LOGINS	 PAYMENTS
 <b>ATTACK RATE</b>			
 <b>OVERALL</b>	3.5%	0.4%	1.9%
 <b>DESKTOP</b>	<b>6.2%</b>	0.3%	1.9%
 <b>MOBILE BROWSER</b>	2.6%	<b>0.5%</b>	<b>2.2%</b>

# LIFE INSURANCE: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Protecting Life Insurance Policies and Products Across the Customer Lifecycle is Critical to Preventing Fraudulent Account Takeover

Life insurance providers operate in a similar way to financial services providers, with provision of wealth management, annuities, mutual funds and well as life insurance products. Many also provide management of tax-free retirement savings programs.






Many of these products and business lines are managed by separate business units, making exposure to risk a key challenge. Organizations need to prioritize a single view

of the customer across all areas of investment in order to build trust and identify anomalous behavior in real time.

As organizations move to unify the consumer experience across lines of business, account sign up and login processes are improving, meaning that identity verification and authentication strategies are key. It is business critical to ensure funds are protected and not exposed to potential account takeovers via attacks on login transactions.

## Key Identity and Access Management and Fraud Challenges that Life Insurers Face:

- Streamlining the onboarding process to remove some of the administrative burden on customers.
- Reducing the risk of fraudsters registering new accounts with stolen or spoofed identity credentials.
- Recognizing returning customers even when they log in to their account infrequently.
- Preventing account takeover attempts from fraudsters attempting to steal funds and balances.

ATTACK RATE	 NEW ACCOUNT CREATIONS	 LOGINS
 OVERALL	0.4%	1.1%
 DESKTOP	<b>0.4%</b>	<b>1.4%</b>
 MOBILE BROWSER	0.2%	0.8%



# 06 CONCLUSION

# CONCLUSION

The outlook for the next six months remains uncertain: while many regions are looking forward to re-building societies and economies ravaged by the effects of COVID-19, global governments remain in a fight between vaccine success and growing virus rates. The need to balance social recovery with economic stability represents a critical path to tread.

This uncertain environment has a profound impact on consumer behavior and the ability to work, travel and socialize freely. For many people, current restrictions mean that working from home, isolating, quarantining and interacting less with colleagues and loved ones remains the norm. This means that fraud and risk models built on current user behavior will have to be continually updated as patterns of interaction change throughout the remainder of the year.

Digital businesses also face a moment of truth when it comes to fraud rates. Where fraud had been so heavily targeted on COVID-related stimulus packages and related scams, how will this approach evolve as

support is wound up and economies start to rebuild? Will fraudsters start to capitalize on the fruits of their bot labors and use validated credentials in higher-volume human-initiated attacks? Will scams, targeting vulnerable and new-to-digital customers, continue to proliferate? How vulnerable will new payment methods and digital platforms – such as buy-now-pay-later – become in the face of economic uncertainty?

Those businesses that succeed and thrive in the midst of this uncertainty will be those that shore up their fraud defenses without impacting customer experience. This means having the ability to track current and evolving consumer behavior across the online customer journey, using intelligence from every interaction to better identify, model and predict future trust and risk.





07

# 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 a purpose of disrupting incumbent financial systems and corporations that rely less on software.

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

**Media** includes social networks, content streaming, gambling, gaming and online dating sites.

## 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 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 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 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.

## 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 uniting offline behavior with online intelligence. LexID Digital has 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 January – June 2021, 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.

## Fraud Network Linking

- Fraud performance data is taken from February to April 2021, based upon devices, email addresses and telephone numbers recorded as fraudulent in the Digital Identity Network.
- Monetary exposure calculated on observed payment transactional value at risk February to April 2021, based upon the identification of all transactions associated with that confirmed fraudulent transaction (and associated group of entities) during the period. 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 January-June 2021 was 34.2 billion.

The LexisNexis® Risk Solutions 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 28.7 billion transactions.

The Cybercrime Report uses these 28.7 billion transactions to calculate overall transaction volumes globally and by region. There are 960K 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 28.7 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 24.7 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.



**FOR MORE INFORMATION:**

[risk.lexisnexis.com/  
FraudandIdentity](http://risk.lexisnexis.com/FraudandIdentity)

[risk.lexisnexis.com/insights-  
resources/research/  
cybercrime-report](http://risk.lexisnexis.com/insights-resources/research/cybercrime-report)

[risk.lexisnexis.com/products/  
threatmetrix](http://risk.lexisnexis.com/products/threatmetrix)

**North America:**

+1 408 200 5755

**EMEA:**

+44 203 2392 601

**LATAM:**

Brazil: + 0800 892 0600

Colombia: +01 800 5 1 84181 or

+57 1 2911359

Mexico: +8000 624 989

All Other LATAM & Caribbean  
countries: +001 855 441 5050

**APAC:**

+852 39054010

**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.

LexisNexis, the Knowledge Burst logo and LexID are registered trademarks of RELX Inc. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Emailage is a registered trademark of Emailage Corp. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2021 LexisNexis Risk Solutions Group. NXR15076-00-0921-EN-US

**For more information, please visit  
[risk.lexisnexis.com](http://risk.lexisnexis.com), and [relx.com](http://relx.com)**