LexisNexis®
RISK SOLUTIONS

THE CHANGING FACE OF CYBERCRIME

The LexisNexis® Risk Solutions Cybercrime Report
January-June 2020

01 INTRODUCTION

Opportunity and Risk in a New Digital Environment

TABLE OF CONTENTS

INTRODUCTION: OPPORTUNITY AND RISK IN A NEW DIGITAL ENVIRONMENT

January to June 2020 has seen societal change on a global level, as COVID-19 continues to impact the global digital economy, regional economies, industries, businesses and consumer behavior.

Online transaction volumes in the LexisNexis® Digital Identity Network® continue to grow, particularly across online retailers and digital banking services. However, some sub-industries have experienced a sharp decline in online transactions as demand for products and services fell due to lockdown restrictions.

The Digital Identity Network® tracks these changes in consumer behavior, collecting and processing global shared intelligence from billions of online transactions across the customer journey, giving businesses an enhanced view of trust and risk.

From January to June 2020, the Digital Identity Network also saw a growth in transactions from new devices, as well as new digital identities, with many new-to-digital consumers moving online to procure goods and services that were no longer available in person, or harder to access via a physical store. This contributed to an overall growth in good customer traffic, as is evidenced in the overall decline in attack volume.

While shifting consumer behaviors and an unstable economic environment have impacted transaction patterns, so too have they changed the face of global cybercrime. Despite this state of flux, however, the Digital Identity Network provides organizations with consistent protection against new and evolving attack vectors. Against a backdrop of fraudsters targeting state-backed financial support packages on a mass scale, the human initiated attack rate in the Digital Identity Network has declined.

It may be that with new lines of COVID-19-related credit to attack, traditional targets – particularly those with robust and established security protocols - have been attacked less. Online fraud is still rife, but it may just be targeting new and emerging products and services, and easier targets. This is supported by the fact that the Federal Bureau of Investigation (FBI) has reported that its Internet Crime Center has already received almost as many fraud reports for 2020 as for the whole of 2019.*

However, while human-initiated attacks targeting financial services and e-commerce have declined, automated bot attacks targeting financial services have grown. The media industry has seen a small growth in the human-initiated attack rate year-over-year.

In addition, new account creations remain a key target for fraudsters looking to register for new products and services, and the attack rate for new account creations from mobile devices has also grown.

As COVID-19-related financial support is reduced, it's possible that many digital businesses that have seen lower attack rates will experience a resurgence in online fraud. Key attack typologies of the last few years will likely persist; mass scale automated bot traffic testing stolen identity credentials, hyperconnected fraud networks operating across industries and organizations, and scams leveraging COVID-19-related anxieties to prey on vulnerable customers.

A growth in new-to-digital customers and a tough economic climate could make these attacks more widespread and diverse, with evidence of mule activity already increasing as mule herders capitalize on economic downturns to recruit new mule accounts into their network.

Businesses must be armed with fraud defenses that layer multiple solutions to detect and block the full spectrum of attacks. These must be future-proofed, evolving as cybercrime moves across geographies, industries, organizations and customers. This relies on differentiating good trusted users - whether new-to-digital or long-established - from potential threats in near real time, before, during and after a transaction is processed.

** www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic*

THE CHANGING FACE OF CYBERCRIME

A Summary of Evolving Threats at a Global, Industry and Regional Level

A Global View

- The media industry experienced a 3% growth in attack rate year-over-year: the only industry to record a growth in overall attack rate. This growth is solely recorded across mobile browser transactions.
- Financial services organizations experienced a growth in automated bot attacks year-over-year and continue to see more bot attacks than any other industry. Global, automated bots remain a key feature of attacks in the Digital Identity Network, contributing to large peaks in the LexisNexis® Risk Solutions Identity Abuse Index.

Across the Customer Journey

- New account creations continue to be attacked at a higher rate than any other transaction type in the online customer journey, although the largest volume of attacks target online payments. Login transactions have seen the biggest drop in attack rate year-over-year in comparison to other use cases.
- Analysis across new customer touchpoints in the online journey has been included in this report for the first time, providing additional context on key points of risk such as password resets and ad listings.

During COVID-19

- The impact of COVID-19 has been felt across all industries, with peaks and troughs in transaction volumes coinciding with global lockdown periods. Financial services organizations have seen a growth in new-to-digital banking users, a changing geographical footprint from previously well travelled consumers, as well as a reduction in the number of devices used per customer. There have also been several attacks targeting banks offering COVID-19-related loans.
- E-commerce merchants have seen a growth in digital payments, as well as several key attack typologies that coincide with the lockdown period. These included account takeover attacks using identity spoofing, and a growth in first-party chargeback fraud.

THE CHANGING FACE OF CYBERCRIME

A Summary of Evolving Threats at a Global, Industry and Regional Level

An Industry View

- The overall attack rate across the financial services and e-commerce industries was reasonably stable from January-June 2020.
- In contrast, the media industry saw several spikes in attack rates coinciding with the COVID-19 lockdown period. This is evidenced in the LexisNexis® Identity Abuse Index for media.
- The financial services industry experienced more login and payment attacks than any other industry. The media industry experienced more new account creation attacks than any other industry.

A Regional View

- LATAM experienced the highest attack rates of all regions globally, with some significant peaks in attacks recorded March-June 2020. Brazil and Mexico have also moved up the list of countries that contribute the largest volume of cyberattacks.
- APAC continues to experience higher attack rates than North America or EMEA, with some significant bot activity recorded coming from Japan, India and Australia.

02

THE CHANGING FACE OF CYBERCRIME:
A GLOBAL VIEW

Click here to watch a short video summary of the **Global HIghlights.**

Global Highlights:

TRANSACTIONS

37% ▲
growth in global transaction volume year-over-year:

36%
growth in financial services transactions.

49%
growth in e-commerce transactions.

13%
growth in media transactions.

ATTACKS

33% ▼
decline in human-initiated attack rate year-over-year:

23%
decline in financial services attack rate.

55%
decline in e-commerce attack rate.

3%
growth in media attack rate.

Mobile browser transactions see the highest attack rate of all channels at 2.4%, despite a decline in attack rate year-over-year.

38%
growth in bot volume targeting financial services organizations year-over-year.

32%
growth in bot volume targeting e-commerce merchants, January-June 2020, in comparison to the previous six-month period.

GLOBAL TRANSACTION PATTERNS IN NUMBERS

Transactions Continue to Move Further Towards Mobile

TRANSACTIONS

The volume of transactions processed by the Digital Identity Network continues to grow consistently year-over-year. This is because:

- More services are moving online.
- New-to-digital users continue to migrate online.
- Existing users transact more as the provision of online services continues to improve and refine.

In addition, there has been a higher take-up of online services as physical stores close due to COVID-19.

The percentage of transactions that are carried out through a mobile device also continues to grow. At the beginning of 2015, just over 20% of transactions in the Digital Identity Network came from a mobile device. In 2020, 66% of all transactions come from mobile devices, largely driven by full service mobile apps.

TRANSACTIONS PROCESSED

22.5B

Growth YOY
+37% ▲

TRANSACTIONS SPLIT BY

Desktop / **Mobile**

34% **66%**

Growth YOY
+6% ▲

Mobile Browser / **Mobile App**

29% **71%**

Growth YOY
+1% ▲

GLOBAL ATTACK PATTERNS IN NUMBERS

Growth in Bot Volume Despite Decline in Human-Initiated Attacks

ATTACKS

HUMAN-INITIATED

ATTACK VOLUME

260M — Decline YOY **-6%** ▼

Attack Split by **Desktop** / **Mobile**

43% 57%

Percentage of attacks coming from mobile devices has increased YOY

+42% ▲

ATTACK RATE

		Decline YOY
Overall	1.4%	-33% ▼
Desktop	1.7%	-50% ▼
Mobile Browser	2.4%	-17% ▼
Mobile App	0.6%	-14% ▼

AUTOMATED BOTS

ATTACK VOLUME

868M — Growth YOY **+13%** ▲

		Growth/ Decline YOY
Financial Services	534M	+38% ▲
E-Commerce	206M	-13% ▼

However, e-commerce did experience a **32% growth** in bot attack volume January-June 2020 in comparison to the previous 6 months.

Media	128M	-5% ▼

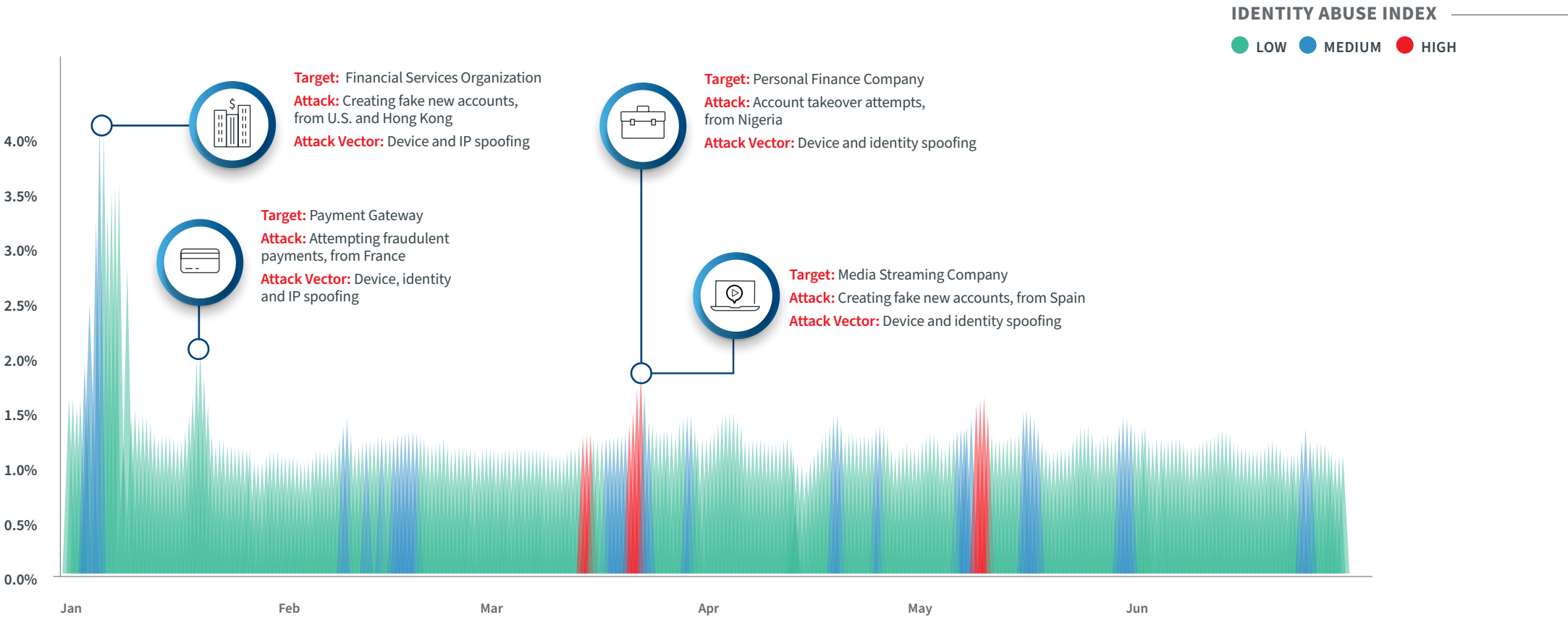
Attacks in the Digital Identity Network are split by human-initiated attacks, which typically return full digital identity profiling data relating to individual events, and high velocity automated bot attacks.

IDENTITY ABUSE INDEX

Despite Early Bot Activity, H1 2020 Shows a More Benign Attack Period Overall

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

KEY ATTACK PEAKS TARGETING FINANCIAL SERVICES ORGANIZATIONS



An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations across a rolling 3-week period.

LexisNexis® RISK SOLUTIONS

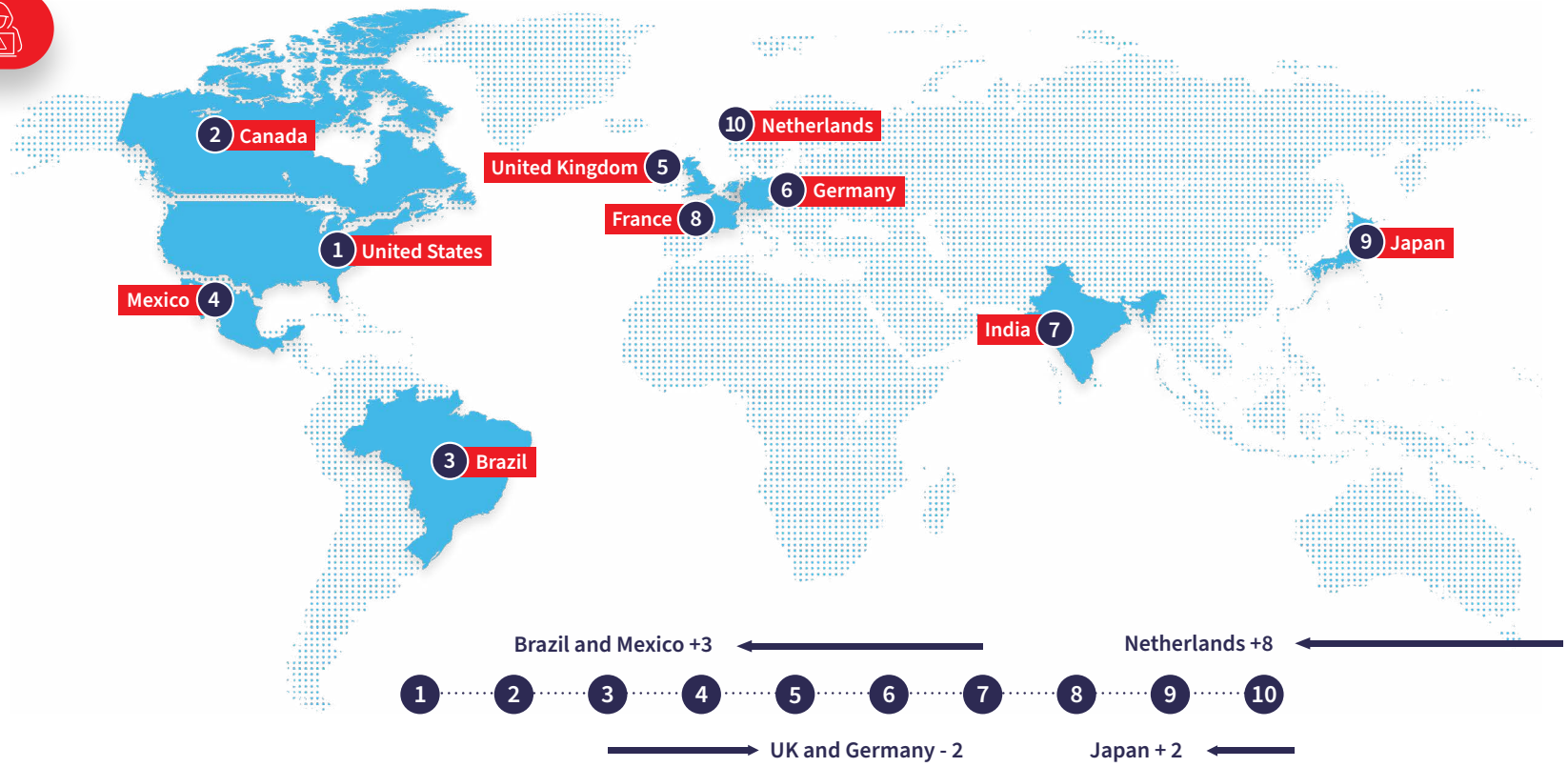
LARGEST CONTRIBUTORS TO HUMAN-INITIATED CYBERATTACKS, BY VOLUME

Japan and Netherlands Join List of Top 10 Global Attackers by Country of Origin

Human-Initiated Cyberattacks

In comparison to the same period last year:

- Brazil and Mexico have both moved 3 places up the top attackers list.
- Japan has moved 2 places up the list.
- Netherlands has moved 8 places up the list.
- UK and Germany have both moved 2 places down the list.



LARGEST ORIGINATORS OF AUTOMATED BOT ATTACKS, BY VOLUME

Japan Records Largest Growth in Bot Attack Originations, Year-Over-Year

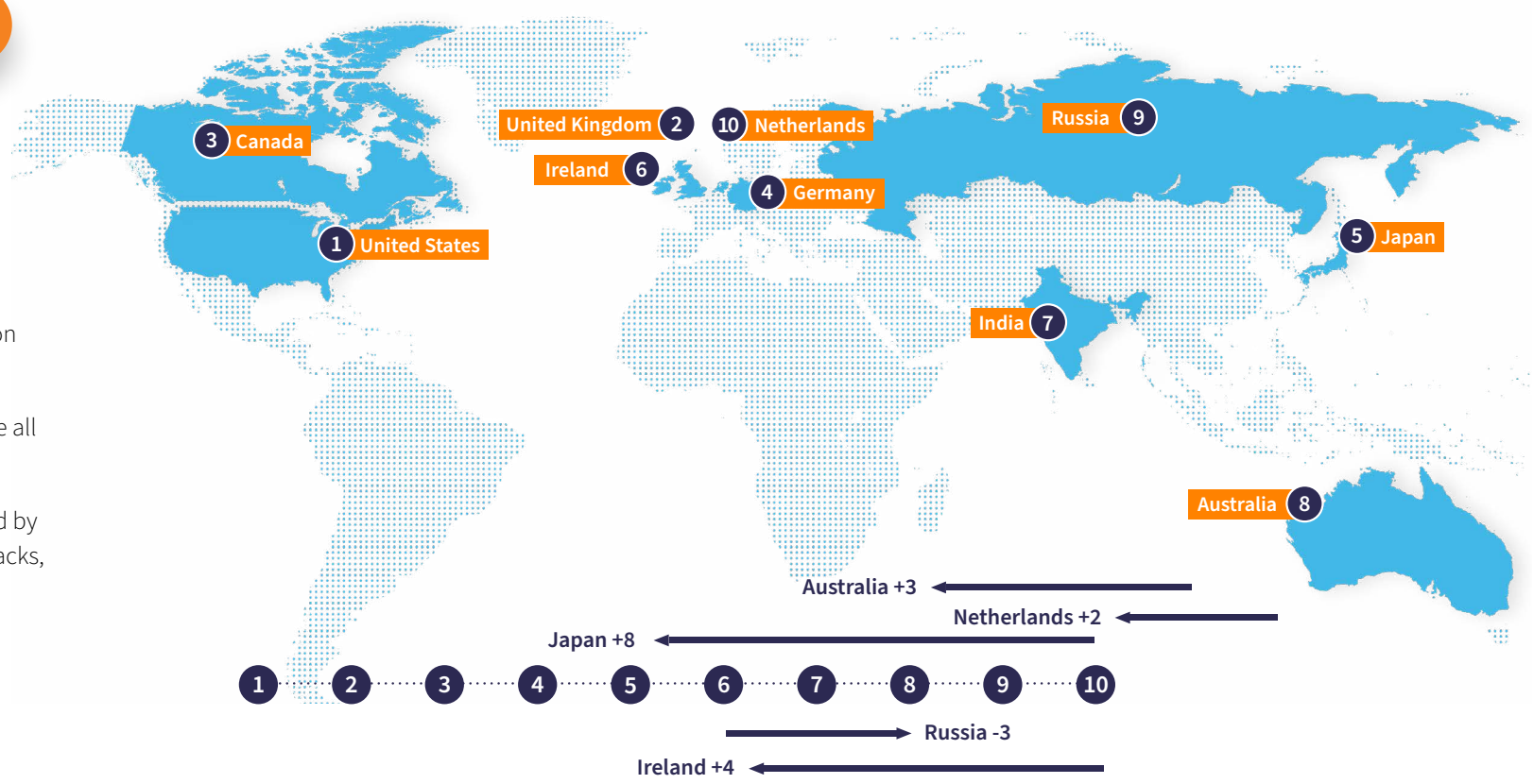
Automated Bot Attacks

LATAM countries that appear in the top human-initiated attack list are notably absent from the top bot attackers list.

Although the U.S. and Canada are top contributors to global bot attacks, the volume of attacks coming from this region has slightly declined year-over-year.

By contrast, APAC, EMEA and LATAM have all experienced a growth in bot volume.

The financial services industry is targeted by the largest volume of automated bot attacks, which grew 38% year-over-year.



03

THE CHANGING FACE OF CYBERCRIME:

ACROSS THE CUSTOMER JOURNEY

Customer Journey Highlights:

New account creations continue to be attacked at a higher rate than any other use case.

88%
growth in new account creation attacks from a mobile app year-over-year.

26%
growth in new account creation attacks from a mobile browser in comparison to the previous six-month period.

Payments transactions see the highest volume of attacks in comparison to other transaction types.

4%
growth in payment attacks from a mobile app in comparison to the previous six-month period.

Transfers (predominantly representing the movement of money between accounts within the same customer profile), see the highest attack rate of all non-core use cases across the customer journey, followed by password reset.

TRACKING TRUST AND RISK ACROSS THE ONLINE CUSTOMER JOURNEY

New Account Creations Represent Key Point of Compromise

The Digital Identity Network processes data from transactions across the entire customer journey, from the point at which an account is opened, then throughout the lifecycle and management of that account.

New account creations are consistently attacked at the highest rate in comparison to all other transactions, representing the key opportunity to exploit, augment and monetize stolen and spoofed credentials.

- Around 1 in every 7 new account creation attempts tracked by the Digital Identity Network is identified as a potential attack.

Account logins have a low overall attack rate, driven by a high volume of trusted transactions from returning customers. However, financial services organizations see the highest volume of login attacks, as fraudsters seek to take over accounts that provide access to customer savings and investments.

Online payments make up the largest proportion of fraud attempts by volume in the Digital Identity Network, as fraudsters try to cash out stolen credentials with a fraudulent money transfer or payment with a stolen credit card.

Although the primary touchpoints in the customer journey are new account creations, logins and payments, there are several other key moments in the customer journey that can provide additional context for trust and risk decisions.

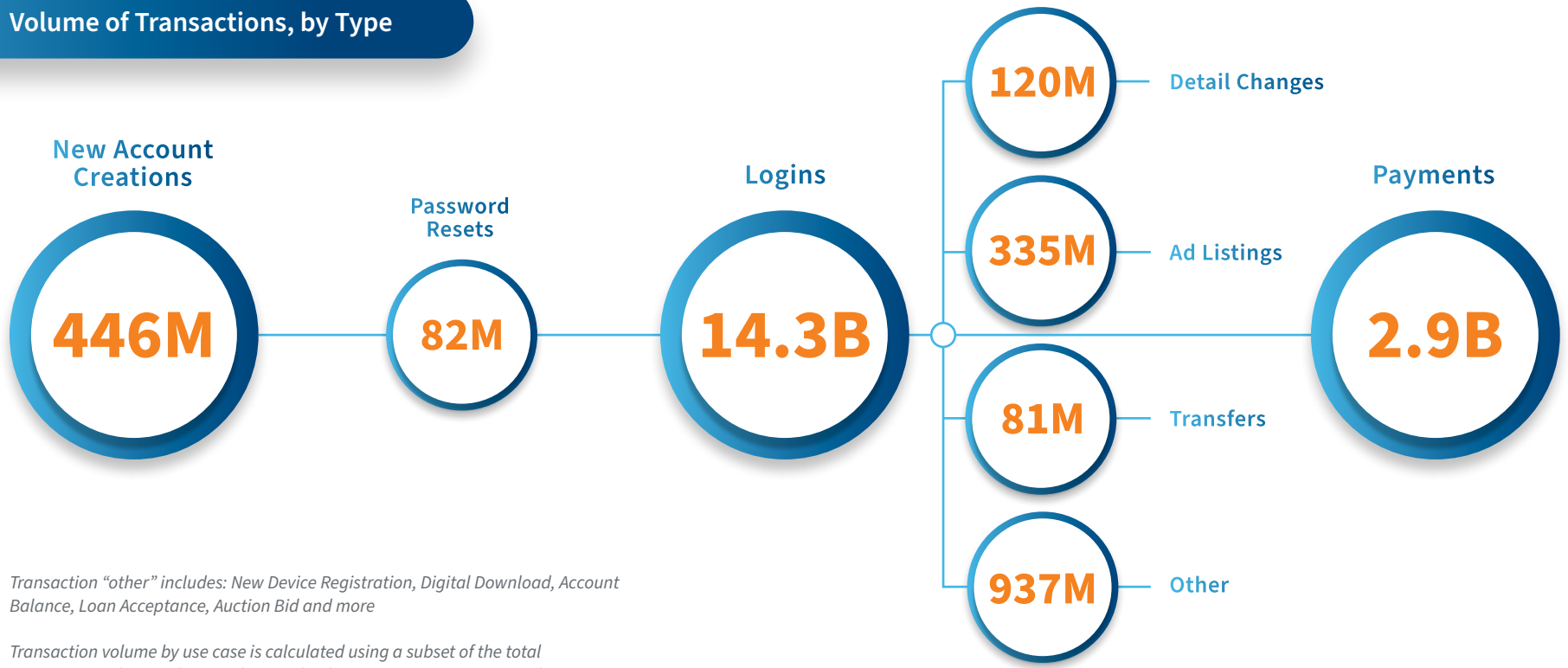
These include account management functions (such as changes to authentication details), or use cases unique to specific industries, (such as ad listings for online marketplaces or reviews for travel companies). Although the attack rate on these subsidiary touchpoints is lower than those on the core touchpoints, these use cases still present significant points of risk in the customer journey, contributing to millions of additional cyberattacks.

Analysis on these additional touchpoints is being introduced for the first time in this report, giving businesses an enhanced view of trust and risk across the entire customer journey, rather than just at point-in-time transactions. High-risk patterns of behavior across multiple online touchpoints can be highly indicative of fraud, that might otherwise be harder to spot. For example, a new account creation at an online marketplace, followed by multiple ad listings tied to that account creation in a short time period, could indicate a potentially fraudulent scenario.

VOLUME OF TRANSACTIONS BY USE CASE ACROSS THE ONLINE JOURNEY

Tracking All Customer Touchpoints for Enhanced Risk Decisioning

Volume of Transactions, by Type



Transaction "other" includes: New Device Registration, Digital Download, Account Balance, Loan Acceptance, Auction Bid and more

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

ANALYZING CORE TOUCHPOINTS

New Account Creations and Payments See Growth in Mobile Attack Rate

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	One-period growth in mobile browser attack rate. Year-over-year growth in mobile app attack rate.	Two consecutive periods of decline in attack rates across all channels.	One-period growth in mobile app attack rate despite decline in other channels.
ATTACK VOLUME	62M	76M	104M
ATTACK RATE			
OVERALL	14.0%	0.5%	3.6%
DESKTOP	15.7%	**1.0%**	3.8%
MOBILE BROWSER	11.1%	0.6%	**3.9%**
MOBILE APP	**19.7%**	0.2%	2.9%

- *One-period growth represents a growth January-June 2020 in comparison to the previous six-month period July-December 2019.*
- *Two consecutive periods of decline represents a decline in the attack rate January-June 2020 in comparison to the previous six-month period, and a year-over-year decline.*
- *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.*

ADDITIONAL HIGH-RISK TOUCHPOINTS

Transfers Experience Highest Attack Rate, Followed by Password Resets

	PASSWORD RESETS	DETAILS CHANGE	AD LISTING	TRANSFER	OTHER
RISK SUMMARY	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.	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 authentication checks, are sent to the fraudster.	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.
ATTACK VOLUME	1.1M	1.0M	1.6M	1.4M	11.5M
ATTACK RATE					
OVERALL	1.4%	0.9%	0.5%	1.8%	1.2%
DESKTOP	**2.0%**	**1.1%**	0.7%	**3.1%**	**1.7%**
MOBILE BROWSER	1.1%	0.8%	**1.5%**	2.2%	0.8%
MOBILE APP	0.2%	0.5%	0.3%	0.9%	0.7%

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.

04

THE CHANGING FACE OF CYBERCRIME:

ANALYZING THE IMPACT OF COVID-19 ON GLOBAL DIGITAL BUSINESSES

Click here to watch a short video summary of the **Impact of COVID-19 Highlights.**

Impact of COVID-19 Highlights:

- Growth in transactions recorded from new devices not seen before in the Digital Identity Network, March to June 2020.
- Growth in new online banking registrations for several financial services organizations, March to June 2020.
- Spike in new account creations for financial services organizations, April to May 2020.
- Evidence of fraud targeting COVID-19-related support packages across several financial services organizations.
- Evidence of an increase in identity spoofing and first-party fraud targeting some e-commerce merchants.

CHANGES IN TRANSACTION VOLUMES THROUGH COVID-19

Analyzing Growth and Decline Across Sub-Industries

As well as looking at the broad industry categories of financial services, e-commerce and media, the Digital Identity Network further categorizes transactions by sub-industry.

From January to June 2020, several periods of growth and decline in transaction volumes were recorded across many sub-industries that have either benefited from, or been negatively impacted by, the effects of COVID-19.

INCREASE IN TRANSACTION VOLUME

- Government Services
- Web Hosting
- Personal Finance
  Some significant growth in lending
- E-Commerce Merchants
  Particularly those selling food and entertainment
- Cryptocurrency
- Digital Wallets
- E-Commerce Marketplaces

DECREASE IN TRANSACTION VOLUME

- Ticketing
  Reliant on live sporting events
- Travel
  Reviews, airlines, accommodation
- Charity
  Heavily impacted by economic / lockdown environments
- Gift Cards
- Gaming and Gambling
- Online Dating

GROWTH IN TRANSACTIONS FROM NEW DEVICES

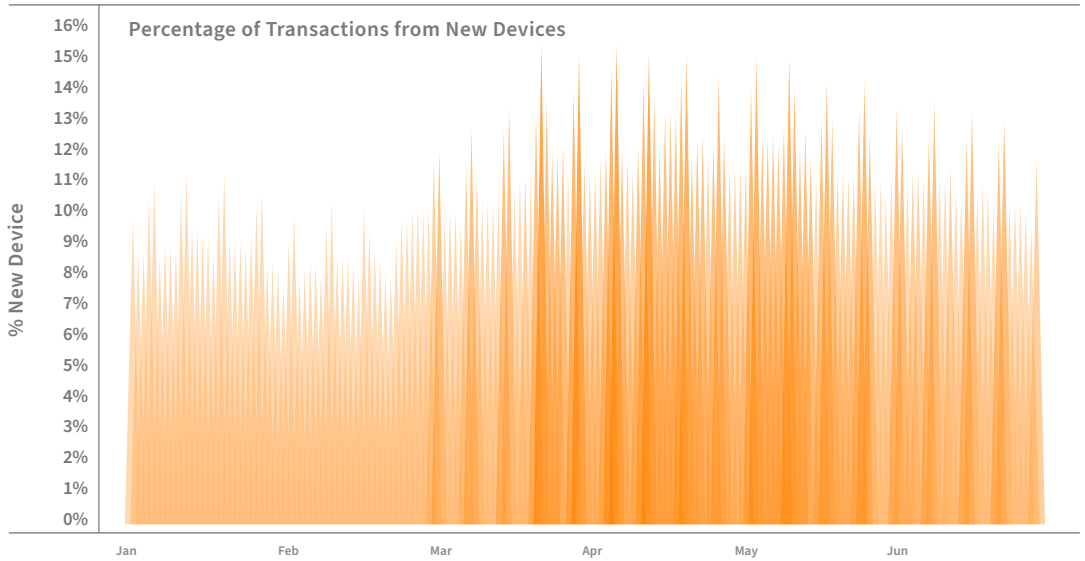
Shift in Global Commerce Draws New Businesses, Users and Devices Online

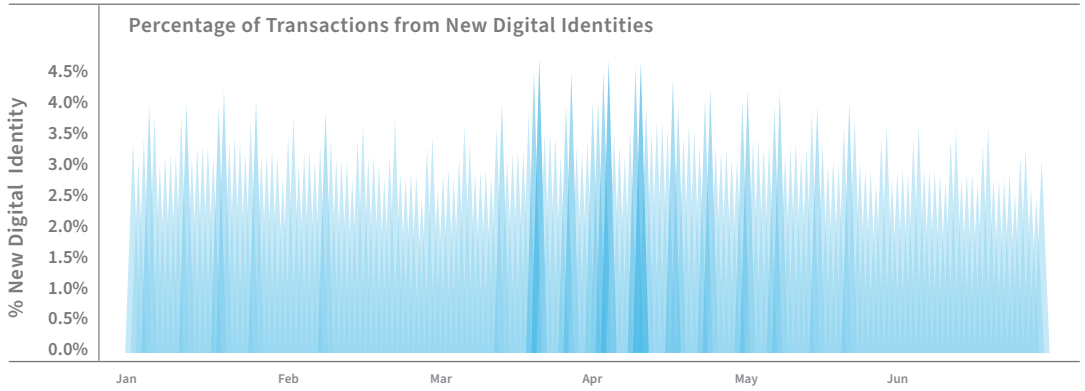
Transactions made with new devices have grown significantly since early March, across all global regions.

Many factors could contribute to this growth, including:

- The lockdown environment changing the way that consumers access goods and services.
- A growth in new-to-digital consumers.
- New organizations looking to protect their online user journey.
- New organizations who have moved their offline functions online.

Some growth was also seen in other new entities, such as digital identity, during March and April.





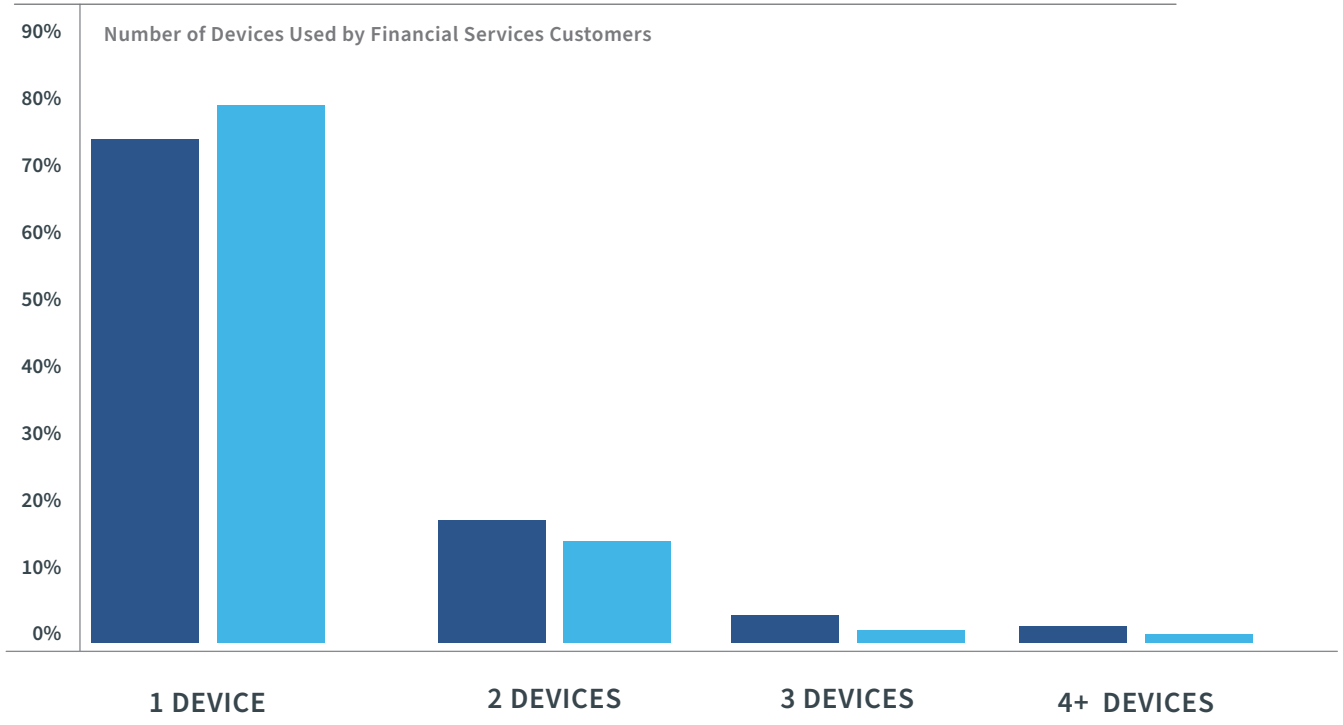
REDUCTION IN NUMBER OF DEVICES USED BY FINANCIAL SERVICES CUSTOMERS

Prevalence of Home Working Sees Consolidation of Device Usage

JAN-20 APR-20

The number of devices used by customers in financial services has reduced as a result of the COVID-19 lockdown.

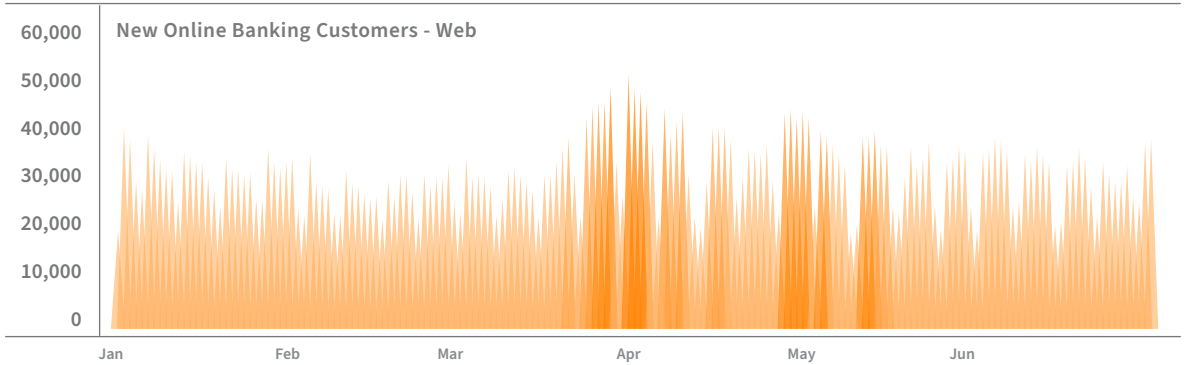
The percentage of customers using one device only has grown between January and April, while the percentage of customers using two or more devices has dropped during the same period.

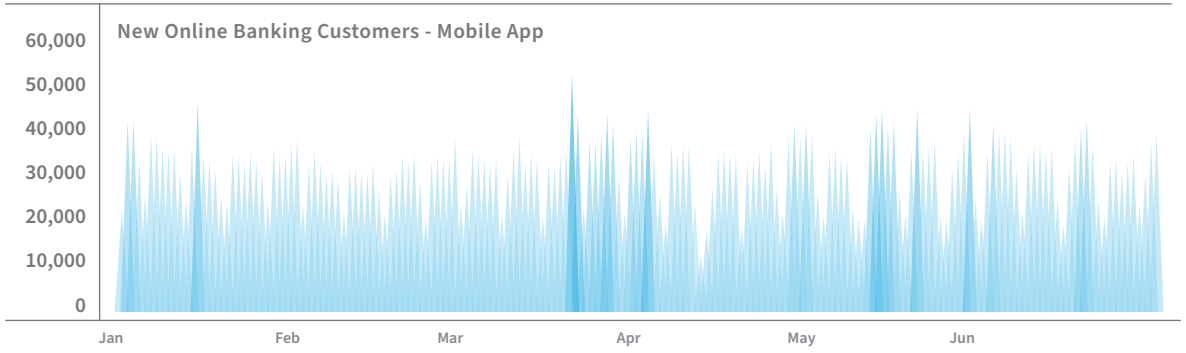


MORE FINANCIAL SERVICES CUSTOMERS TURN TO DIGITAL FOR THE FIRST TIME

Online and Mobile Banking Registrations Grow at Start of Lockdown

Several financial services organizations in the Digital Identity Network saw a growth in new registrations for online banking, both via web and mobile app, at key points throughout January-June 2020.





SIGNIFICANT REDUCTION IN CONSUMER TRAVEL REFLECTED IN LOGIN ACTIVITY

Fewer Logins Recorded for Travelers Across Regions

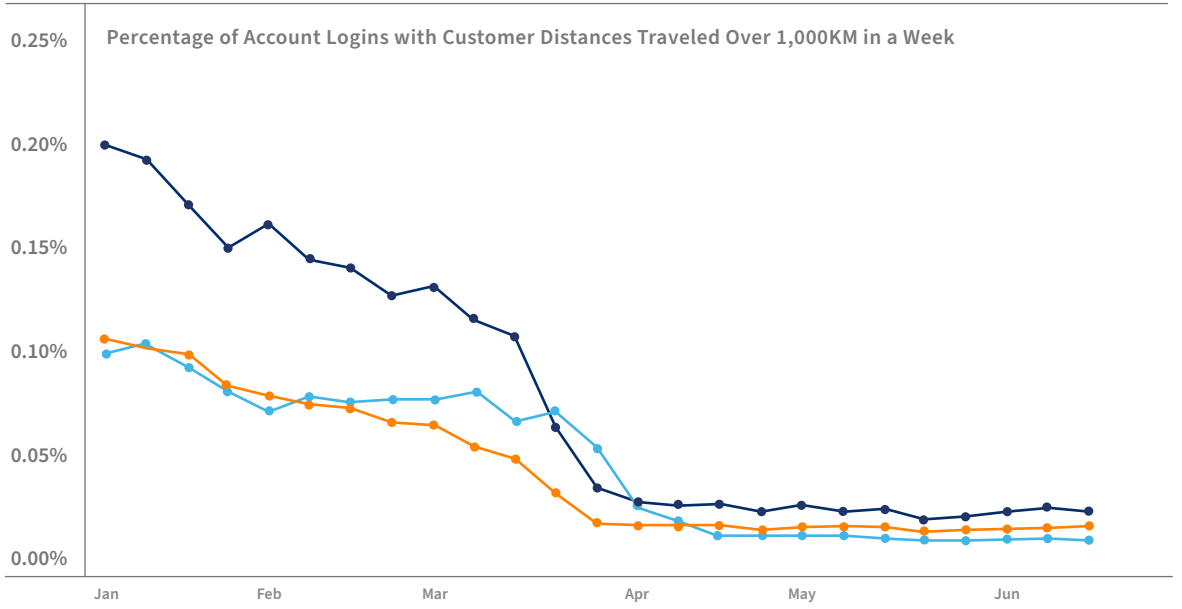
U.S CANADA UK

Both North American and UK financial services institutions recorded far fewer logins from customers that had traveled more than 1,000km in a week.

- Global travel restrictions have meant customers predominantly log in from local locations.

Login patterns also shifted from a high density in urban and metropolitan areas, to a wider dispersal around suburban and rural areas.

- Fewer logins recorded from office locations as more consumers work from home.



GROWTH IN NEW ACCOUNT CREATIONS COINCIDES WITH LOCKDOWN PERIOD AND RELEASE OF FINANCIAL SUPPORT PACKAGES

Spike in Applications Includes Credit Cards, Loans and Deposit Accounts

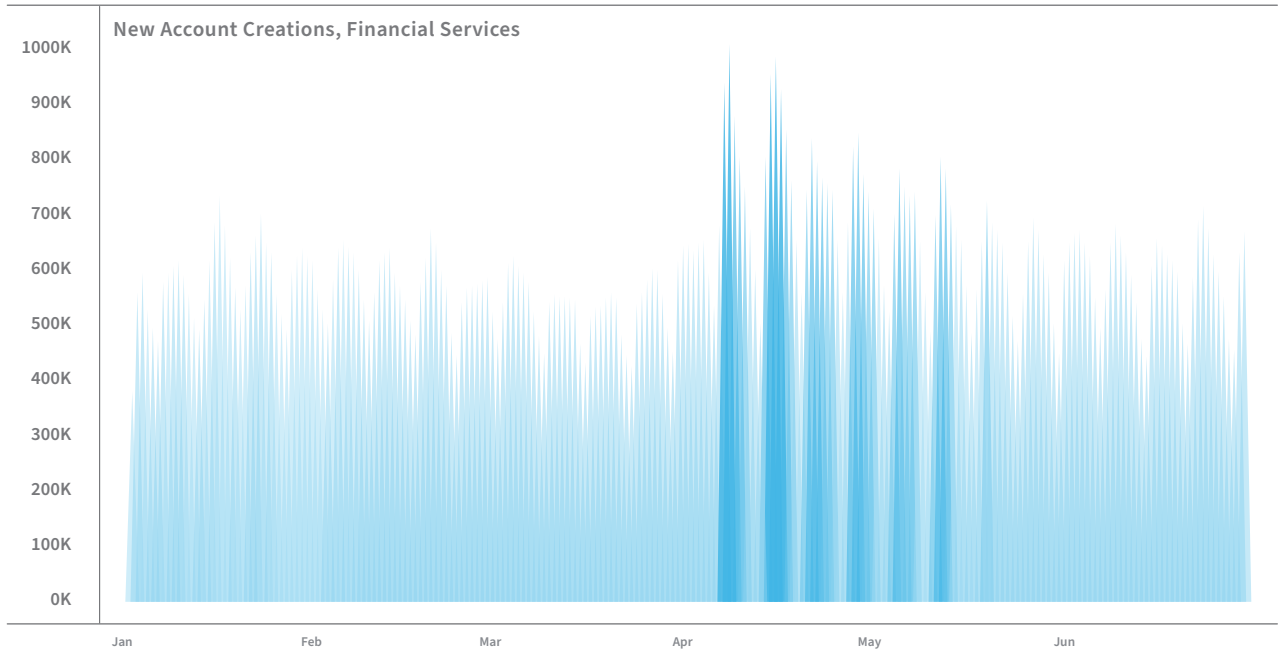
Many countries are offering financial support for both businesses and consumers impacted by the COVID-19 pandemic.

This financial support has had an impact on the transaction volumes of several financial services organizations in the Digital Identity Network.

There has been an overall growth in new account creations for financial services April to May 2020.

These includes a combination of:

- Deposit account applications to pay in government-backed funds.
- Loan applications – where government-backed business loans are administered by the financial services organization.
- Credit account applications for back-up sources of credit during the pandemic.
- New online banking registrations.



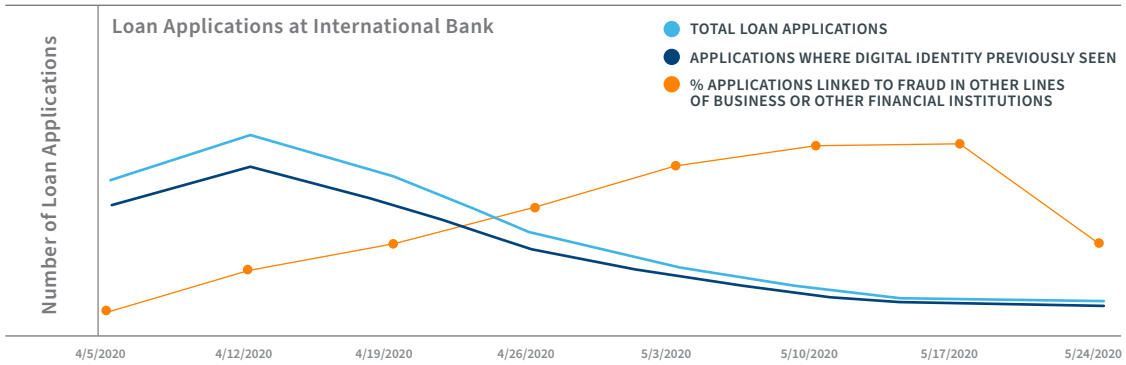
SHARING INTELLIGENCE TO REDUCE THE RISK OF FRAUD DURING COVID-19

International Bank Uses Intelligence from the Digital Identity Network to Mitigate Risk for COVID-19 Loan Applications

This international bank has implemented LexisNexis® ThreatMetrix® on its new COVID-19-related online loan application as an additional layer of risk mitigation. These loans are backed by the government to support small business owners in the region.

LexisNexis ThreatMetrix can help the bank identify high-risk applications in near real time.

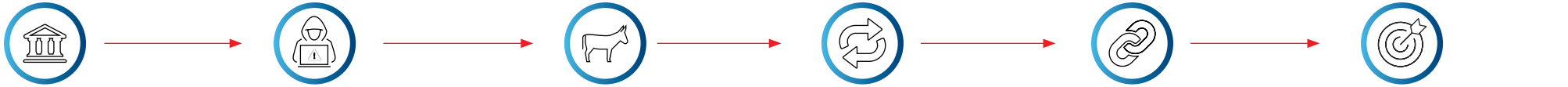
The bank can also benefit from crowdsourced intelligence from other providers, understanding, for example, whether an applicant has been flagged as high-risk elsewhere in the Digital Identity Network.



- More than **80%** of loan applications came from personas previously seen in the Digital Identity Network.
- More than **800** applications linked to fraud on the bank's other lines of business.
- **Approximately 50** applications linked to fraud or compromised credentials at another financial institution in the Digital Identity Network.

SHARING ADDITIONAL DATA POINTS WITH TRUST AND CONTEXT WITHIN CONSORTIUM

UK Banking Consortium Shares Data Relating to Fraudulent Loan Applications



The UK banking consortium has seen an increase in fraudulent activity on new loan applications for the government-backed Bounce Back Loans Scheme (BBLS) in response to COVID-19.

Fraudsters have used several tactics to try and secure a loan, including:

- Upgrading consumer accounts to business accounts to meet the loan scheme requirements.
- Applying for multiple loans using the same underlying credentials to maximize monetary payout.

Several applications have been linked to known mule activity using link analysis relating to devices, locations and behaviors.

A group of UK banks is sharing information related to confirmed fraudulent loan applications with other members in the consortium, to identify and block fraudsters attempting to defraud multiple UK banks.

Link analysis has been used to identify and track high-risk activity across the banking consortium.

Policy rules have been created to target specific fraudulent patterns of behavior, in near real time.

GROWTH IN ONLINE PAYMENTS AT E-COMMERCE MERCHANTS COINCIDES WITH GLOBAL LOCKDOWN

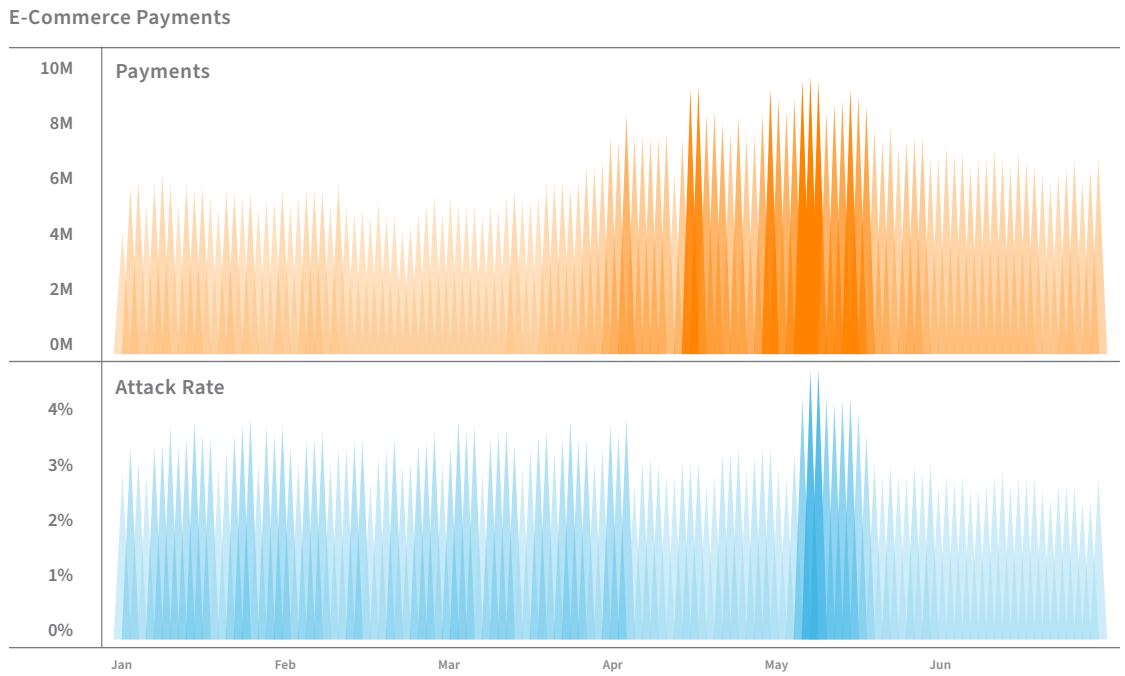
Fall in Payments Attack Rate Indicates a Higher Proportion of Trusted Transactions

E-commerce merchants in the Digital Identity Network saw a strong growth in online payments coinciding with the lockdown period.

Although the e-commerce industry has seen some pockets of attack growth, the payments attack rate is on a general downward trend. This indicates that much of this growth in payment transaction volume came from trusted customers, who were turning to online platforms in place of physical stores.

However, there was a spike in attack rates during May; with the highest attack rate of the period recorded at 4.6%.

This was predominantly caused by an identity spoofing attack coming from Brazil, targeting a global payments gateway.



FRAUDSTERS TARGET E-COMMERCE LOGINS WITH IDENTITY TESTING BOTS

Large Merchant is Key Target for Identity Spoofing Account Takeovers

FRAUD:
Sustained increase in login attack rate April to June 2020, possibly coinciding with the lockdown period when fraudsters knew consumers were making more online transactions.

TARGET:
U.S. e-commerce merchant.

METHOD:
Automated bots testing stolen identity credentials.

ATTACK:
Global bot attacking from several locations including US, Russia, Vietnam and Japan.

DETECTION:
Multiple login attempts made from the same device / location during a short period of time.

EMAIL ADDRESS INTELLIGENCE PROVIDES ADDITIONAL RISK CONTEXT DURING COVID-19

Growth in High-Risk Activity Related to Chargebacks and Shipping Fraud

LexisNexis® Emailage® uses email address metadata, along with customer name, location data, shipping / billing address and phone number, as a basis for transactional risk assessment and digital identity validation.

Intelligence from LexisNexis® Emailage® March – June 2020, augments analysis from the Digital Identity Network to reveal additional insights regarding potential fraud risks as a result of COVID-19.

These include:

A growth in first-party chargeback fraud as more consumers attempt to claim money back for goods they actually received.

A growth in fraud linked to email addresses that had multiple billing addresses associated with them in a short time frame.

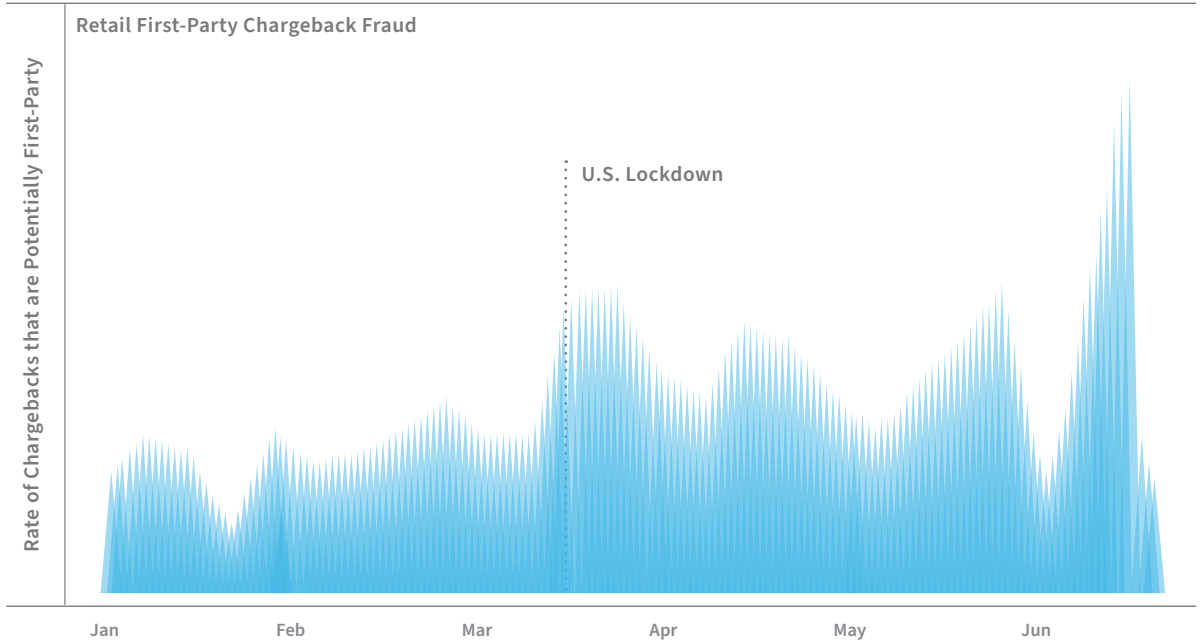
During lockdown, since more customers are transacting near or from home, there is an increase in the likelihood of fraud when the distance between IP and billing address is large.

1. LINK BETWEEN CARD-NOT-PRESENT TRANSACTION AND EMAIL DATA SHOWS INCREASE IN FIRST-PARTY CHARGEBACK FRAUD RATE

Analysis Suggests Consumers are Claiming More Chargebacks for Goods they Received During Lockdown

Analysis shows a strong pattern of growth in first-party chargeback fraud for a U.S. e-commerce merchant.

This analysis validated that both the transactions and the chargebacks were likely coming from the legitimate owner of the credit card, based on a digital identity confidence score.



2. GROWTH IN FRAUD LINKED TO EMAIL ADDRESSES WITH MULTIPLE BILLING ADDRESSES

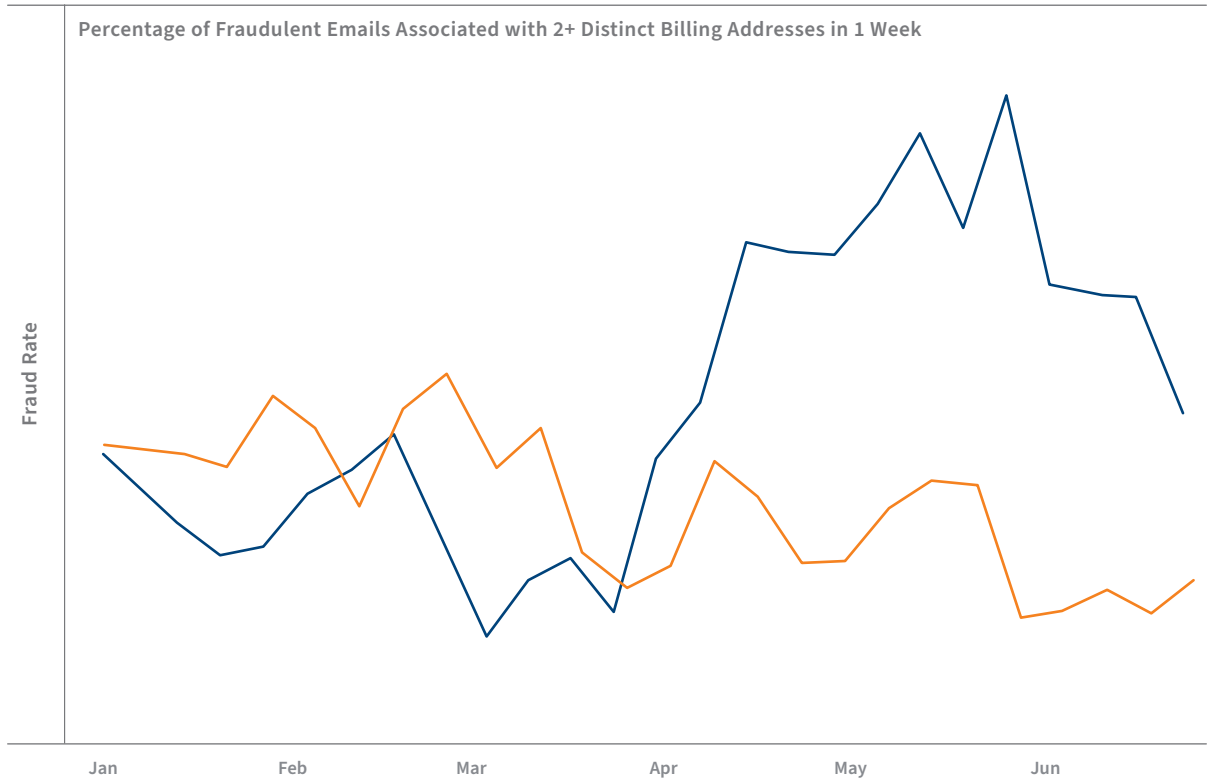
Significant Growth in Fraud Rates Between April to June 2020

FRAUD 2020 FRAUD 2019

A U.S. e-commerce merchant saw a marked increase in fraud relating to emails that had multiple billing addresses associated with them in a short time frame.

In April, **40-50%** of emails that were associated with multiple billing addresses in one week were reported as fraud.

This represents a significant growth in the fraud rate between April to June 2020, as well as a marked increase in fraud in comparison to 2019.



3. INCREASED FRAUD RISK RELATING TO IP AND BILLING ADDRESS DISTANCE DURING COVID-19

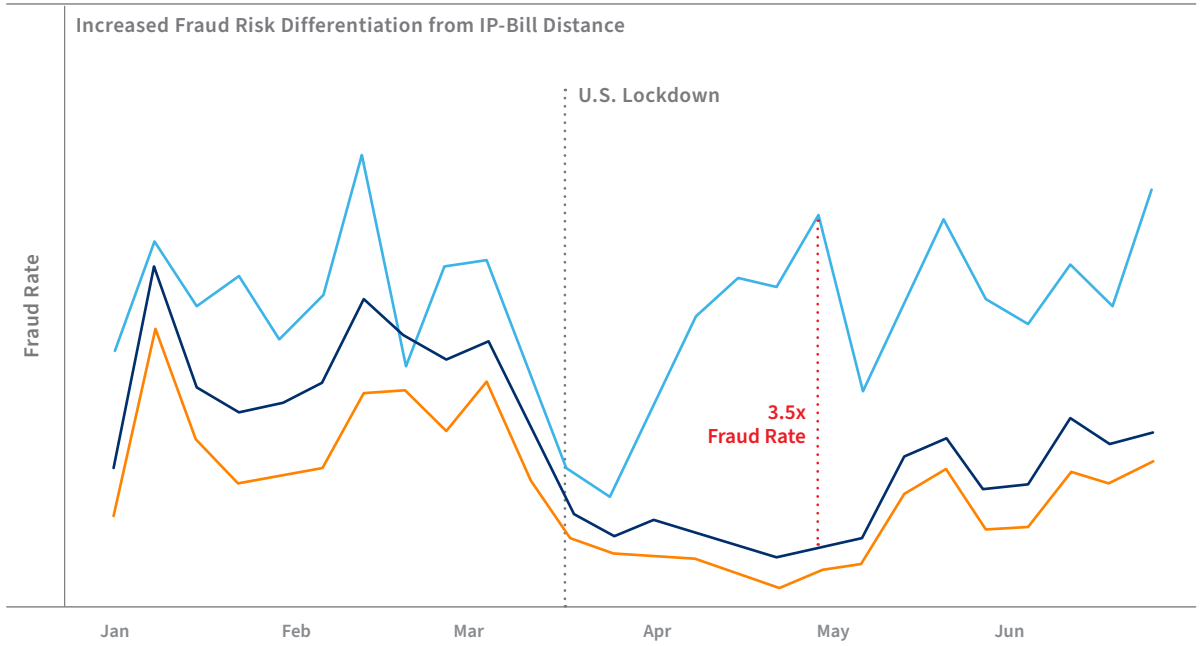
A Reduction in Travel During Lockdown Makes Transactions that were Initiated Further from Billing Address More Indicative of Fraud

OVERALL DIST < = 10 MILES DIST > 1,000 MILES

The overall population is compared to two sub-populations:

- Consumers with IP / billing address distance < = 10 miles (generally low-risk).
- Consumers with IP / billing address distance > 1,000 miles (generally high-risk).

Between April and June, the likelihood that a large distance between IP and billing address was indicative of fraud has increased.



05

THE CHANGING FACE OF CYBERCRIME: AN INDUSTRY VIEW

Industry Highlights:

Financial Services

- The financial services industry saw more login and payment attacks than any other industry.
- New account creations from desktops and mobile apps have seen a two-period growth in attack rate.
- Although financial services payments are attacked at a higher rate than other industries, the attack rate is declining.

E-commerce

- Two-period growth in the attack rate on new account creations from mobile browsers.
- Two-period growth in the attack rate on payments from a mobile app.

Media

- The media industry saw more new account creation attacks than any other industry.
- Media organizations have seen the most noticeable spikes in attack rates as a result of COVID-19, with an increase in attacks recorded March-April 2020.
- Two-period growth in the attack rate on logins from a mobile app.
- Two-period growth in the attack rate on new account creations from a desktop.

FINANCIAL SERVICES: OVERVIEW OF TRENDS AND ATTACK PATTERNS

New Account Creations See Highest Rate of Attack, Which Continues to Grow

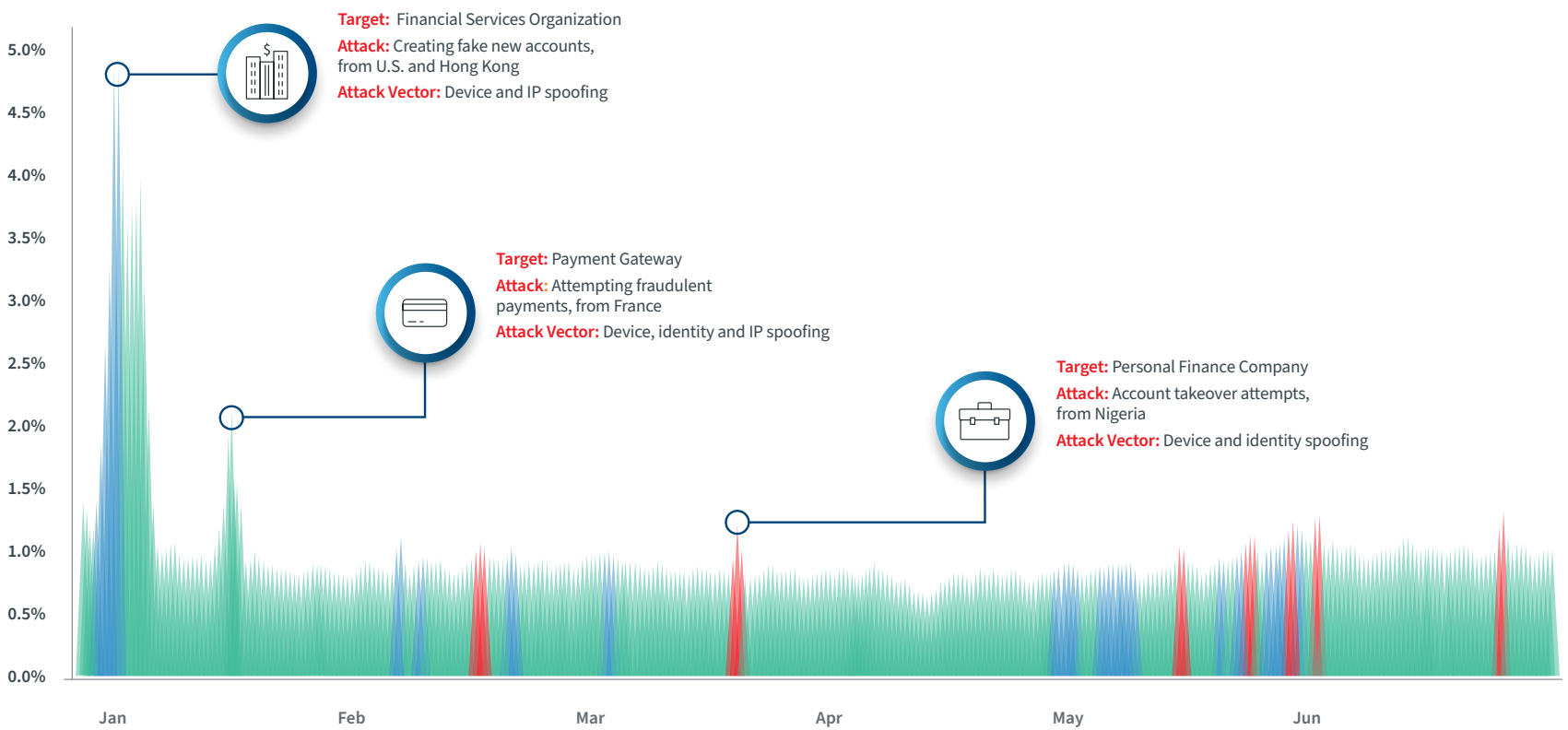
	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Two consecutive periods of growth in attack rates across desktop and mobile app.	Two consecutive periods of decline in attack rates across all channels.	Two consecutive periods of decline in attack rates across all channels.
ATTACK VOLUME	16M	46M	62M
ATTACK RATE			
OVERALL	13.1%	0.4%	4.0%
DESKTOP	6.1%	**0.8%**	4.2%
MOBILE BROWSER	3.2%	0.6%	**5.2%**
MOBILE APP	**29.2%**	0.1%	2.0%

- New account creations and payments are key targets in the financial services customer journey, offering fraudsters the opportunity to monetize stolen credentials and cash out.
- A large bot attack targeting new app registrations in December 2019 continued through January 2020, contributing to the high mobile app attack rate on new account creations.

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

FINANCIAL SERVICES IDENTITY ABUSE INDEX

Large Global Bot Attack Targeting New App Registrations in 2019 Continued Through January 2020



An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations across a rolling 3-week period.

IDENTITY ABUSE INDEX

LOW MEDIUM HIGH

The attack pattern for financial services is characterized by a number of automated bot attacks that contribute to large peaks in the overall attack rate.

Aside from these bots, the attack environment was largely stable with no notable changes to existing trends.

DETECTING NEW ACCOUNT CREATION FRAUD AT BRAZILIAN FINANCIAL SERVICES ORGANIZATION

Mobile Device Attributes Were Used to Identify and Block Fraud Attacks

FRAUD:
Fraudulent new account creations from a mobile device.

TARGET:
Brazilian financial services organization.

METHOD:
Fraudsters attempted to hide the fact they were creating multiple new accounts from the same device by changing device fingerprinting parameters to evade detection.

ATTACK:
Growth in fraud attempts on new accounts opened during March 2020.

DETECTION:

- Almost all the fraud attempts were related to devices that had attempted to evade detection using different forms of device swapping activity.
- Persistent markers indicating that this high-risk activity was coming from the same device helped to identify the fraud.
- Rules that were subsequently enabled by the financial organization were so effective at blocking device swapping routines that they reduced total fraud attempts by 20%.

MITIGATING CASHBACK PROMOTION ABUSE FOR MALAYSIAN DIGITAL WALLET PROVIDER

Fraudsters Use Mule Accounts to Siphon Off Proceeds of Bonus Abuse

FRAUD:
Multiple account creations, logins and initial payment transactions used to exploit new account bonuses.

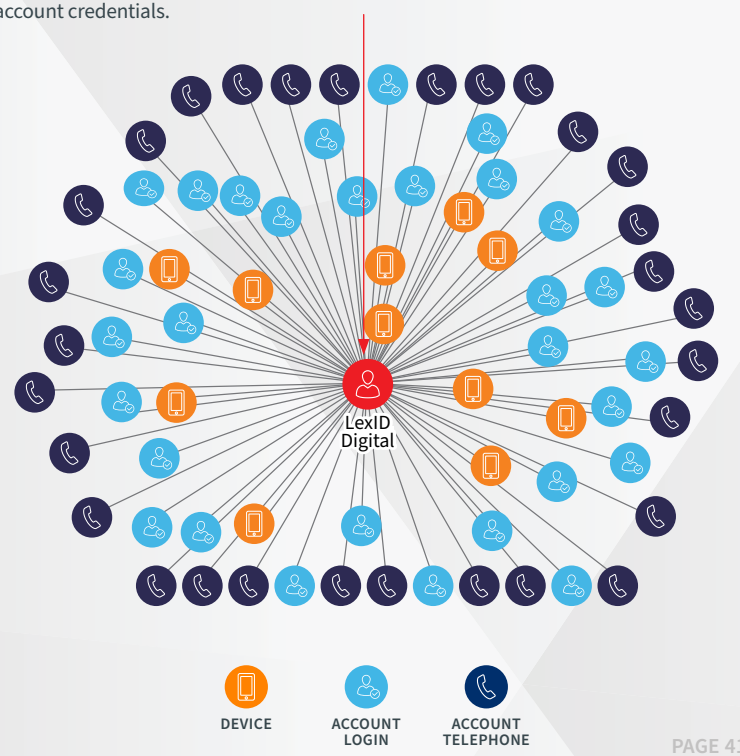
TARGET:
Malaysian digital wallet provider.

METHOD:
Fraudsters set up multiple new accounts from a small number of devices, attempting to bypass device fingerprinting.

ATTACK:
- New account was created.
- First transaction was initiated.
- Cashback promotion triggered by first transaction was immediately transferred to a mule account.

DETECTION:
Multiple accounts created in a short space of time from virtual machines.

One unique LexID Digital® entity indicates a single source of bonus abuse across multiple account credentials.



E-COMMERCE: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Mobile Channel Contributes to Growth in Attack Rates in E-Commerce

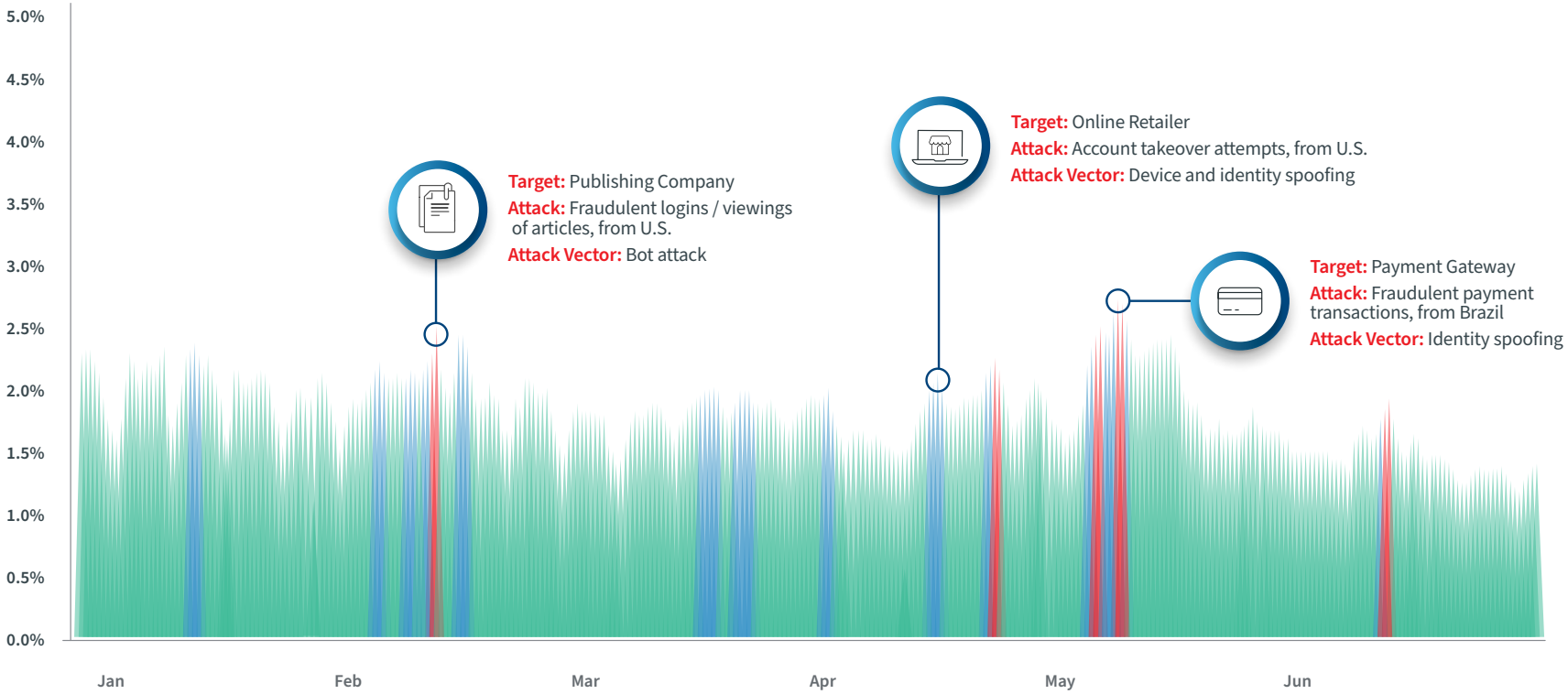
	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Overall decline in attack rates, except on mobile browser transactions which have seen a two-period growth in attack rate.	Decline in attack rates across all channels. This is driven by a decline in attack volume and a higher volume of transactions from trusted customers.	Overall decline in attack rates except on mobile app transactions, which have seen a two-period growth in attack rate.
ATTACK VOLUME	6.5M	22M	39M
ATTACK RATE			
OVERALL	6.9%	1.2%	3.2%
DESKTOP	**11.8%**	**1.6%**	3.5%
MOBILE BROWSER	6.0%	0.6%	2.4%
MOBILE APP	1.5%	0.4%	**4.2%**

- New account creations and payments represent the key risk points in the e-commerce online customer journey.
- Attacks are growing across the mobile channel, specifically on new account creations from a mobile browser and payments from a mobile app.
- Identity spoofing on e-commerce logins is high, with an attack rate of 12% and above for 3 consecutive periods.

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.

E-COMMERCE IDENTITY ABUSE INDEX

Some Spikes in Attack Rates for Specific Merchants and Payment Providers



An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations across a rolling 3-week period.

IDENTITY ABUSE INDEX

LOW MEDIUM HIGH

The attack rate for e-commerce merchants followed similar peaks and troughs across the 6-month period.

A large e-commerce payments provider saw some significant growth in attack activity during May 2020.

There was a noticeable drop in the attack rate mid-May through June.

U.S. MOBILE OPERATOR TARGETED FOR HIGH VALUE HARDWARE

Fraud Ring Attempts to Evade Capture by Operating Across Multiple Devices

FRAUD:
A fraud network targeted this mobile operator in order to place multiple orders for high-value handsets.

TARGET:
U.S. mobile operator

METHOD:

- **Credential testing:** Fraudster tested combinations of stolen credentials at high velocity in order to create a valid new account with the mobile operator.
- **Fraudulent order placement:** Once a successful account had been created, a separate "clean" device placed the order for new hardware.

ATTACK:
Fraud network using a series of high-risk and "clean" devices for a two-staged attack in order to bypass velocity rules and device fingerprinting.

DETECTION:

- Use of dynamic rules to alert the mobile operator to when multiple identity credentials were being tested via one device.
- Conversely, alerting the mobile operator to when multiple devices are associated with one stolen identity.

MEDIA: OVERVIEW OF TRENDS AND ATTACK PATTERNS

All Use Cases Record Growth in Attack Rates Jan-June 2020

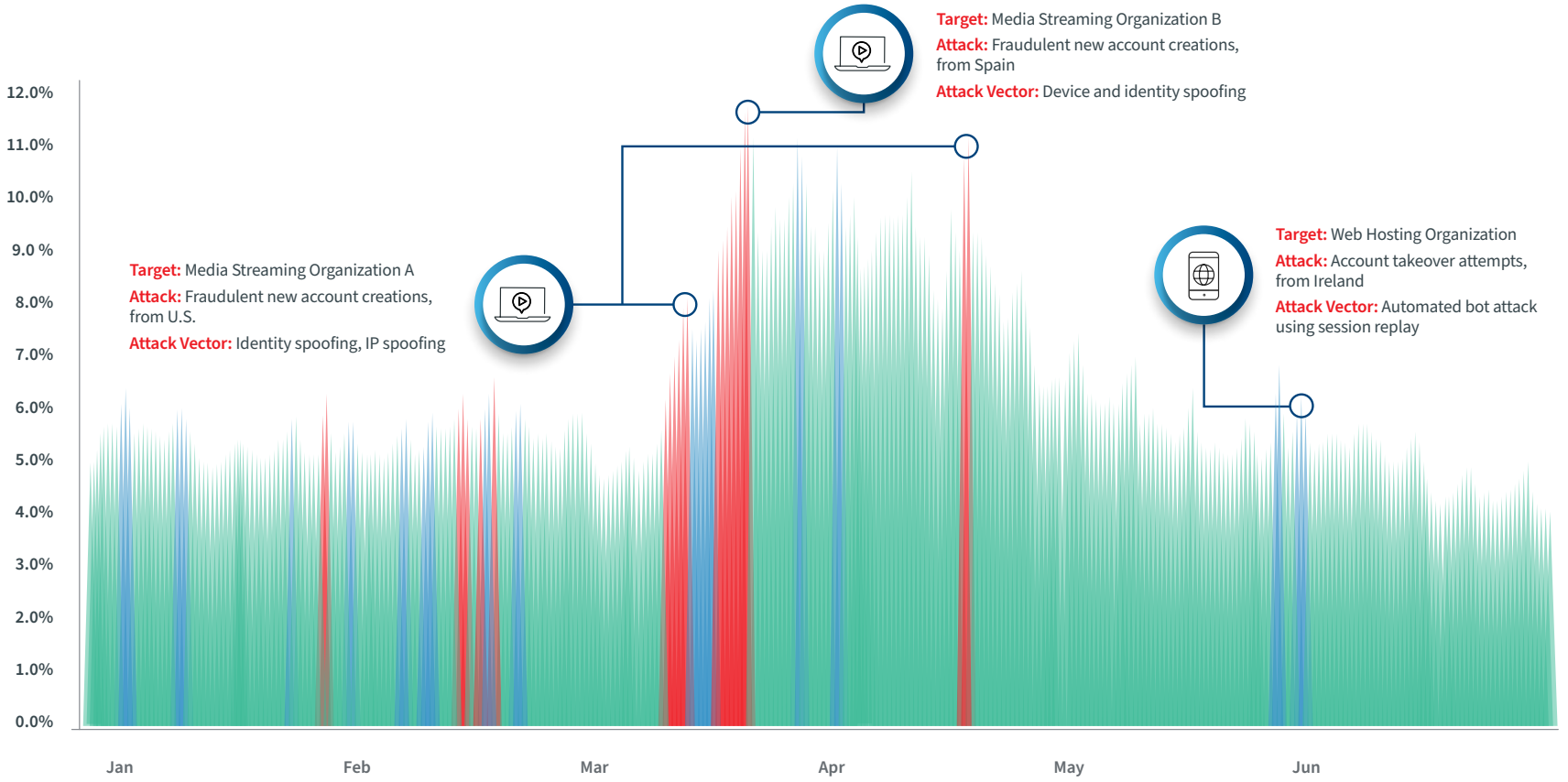
	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Two-period growth in attack rate on desktop transactions. One-period growth in attack rate on mobile browser transactions.	Two-period growth in attack rate on mobile app transactions.	One-period growth in attack rate on mobile app transactions.
ATTACK VOLUME	39.6M	8.2M	3.4M
ATTACK RATE			
OVERALL	17.4%	1.7%	2.9%
DESKTOP	**23.7%**	0.8%	2.7%
MOBILE BROWSER	15.1%	0.5%	2.9%
MOBILE APP	17.1%	**12.8%**	**3.1%**

- Media-based new account creations are attacked at a higher rate than any other industry.
- Globally, identity spoofing is most prevalent in the media industry and specifically on new account creation and payments transactions. Payments particularly seem a prime target, with a two-period growth recorded on the percentage of attacks using identity spoofing.

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.

MEDIA IDENTITY ABUSE INDEX

Sustained Growth in Attack Rate Recorded March-April 2020



IDENTITY ABUSE INDEX

LOW MEDIUM HIGH

The media industry recorded the most noticeable spikes in attack rates during Jan-June 2020, coinciding with several COVID-19 regional lockdowns.

Attack rates were consistently higher in March and April in comparison to January and February.

This was largely driven by an increase in fraudulent activity at media streaming organizations within the Digital Identity Network.

An Identity Abuse Index level of high (shown in red) represents an attack rate of two standard deviations across a rolling 3-week period.

EMEA GAMBLING COMPANY TARGETED BY FINNISH FRAUD RING

Fraudsters Launch Targeted Bonus Abuse Attack

FRAUD:
Criminal gang targeted free bonuses offered for first-time gameplay, in order to increase chances of winning the jackpot.

TARGET:
Large EMEA-based gambling company.

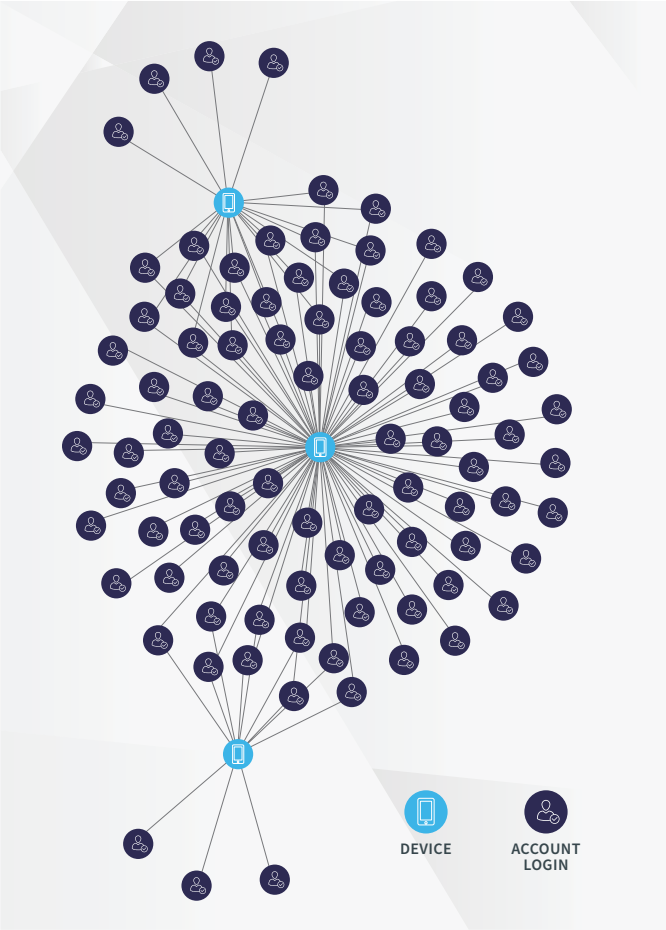
METHOD:
All accounts were offered a free trial of a specific game for 30 days. Creating multiple accounts significantly increased the likelihood of winning the jackpot.

ATTACK:

- 85 accounts were created using "different" devices, from a virtual machine in Finland.
- During April, one device made over 100 login attempts to these accounts.

DETECTION:

- Device markers suggest the account creations came from the same virtual machine.
- Large volume of login attempts from one device.



06

THE CHANGING FACE OF CYBERCRIME: A REGIONAL VIEW

Regional Highlights:

APAC has a high instance of automated bot attacks, with Japan, India and Australia all appearing on the list of top bot originators, by volume. There was a particularly large attack originating from the Philippines in June 2020.

EMEA has the highest penetration of mobile transactions of all regions, with corresponding low mobile attack rates. The desktop attack rate is slightly higher than the global average, however.

LATAM has the highest overall human-initiated attack rate of all regions and saw consistent spikes in attack rates from March to June 2020, which coincided with the onset of COVID-19 in the region.

North America has lower overall attack rates than the global averages, with declining human-initiated and bot attack volumes. However, despite these declines, the region remains the largest contributor, by volume, for both human initiated and bot attacks.

IDENTITY ABUSE INDEX BY REGION

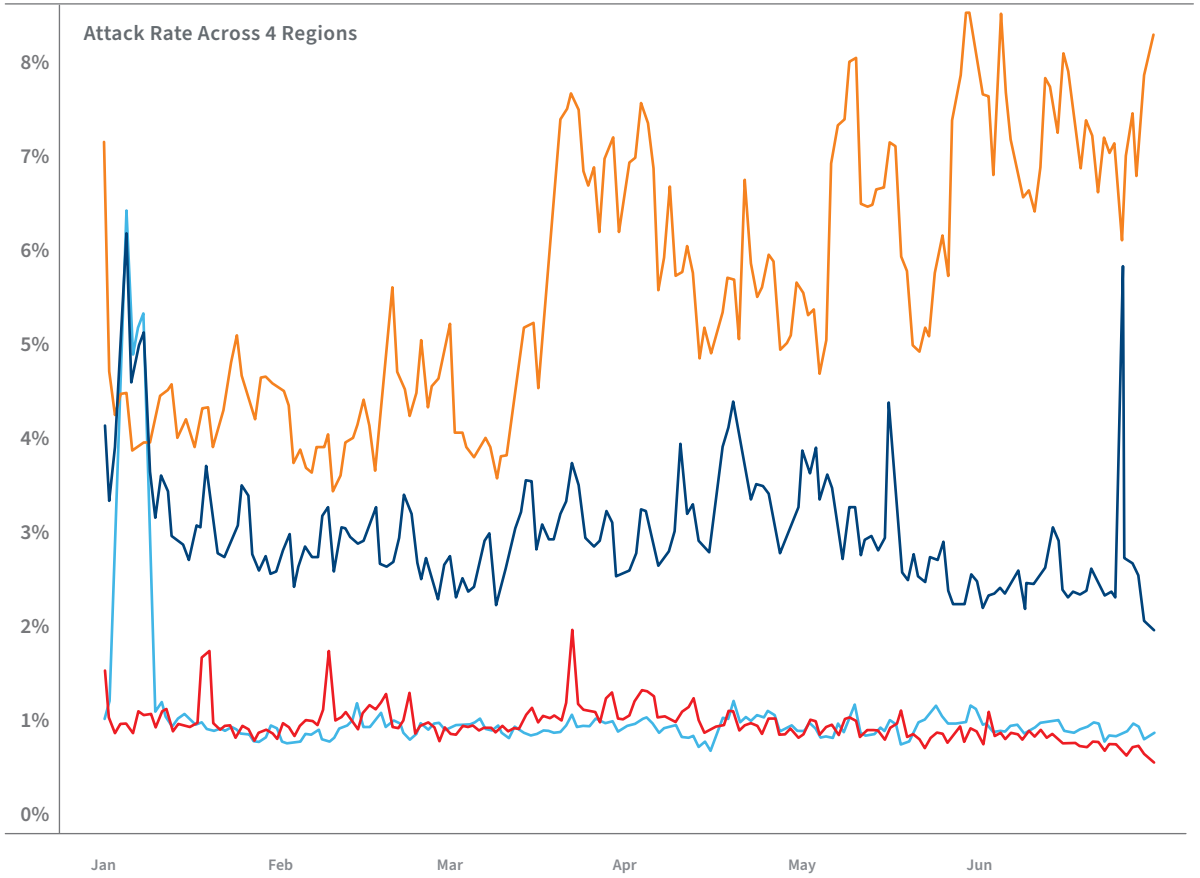
LATAM Sees Largest Spikes in Attack Rates Coinciding with COVID-19

APAC LATAM NORTH AMERICA EMEA

LATAM continues to record the highest attack rates of all regions and has experienced several spikes in attack rates during COVID-19.

APAC saw some growth in attack rates during April and May. The large spike in attack rate in June was an identity spoofing bot attack, originating from the Philippines, targeting a payment gateway.

North America and **EMEA** recorded lower overall attack rates but continued to be targeted by automated bot attacks which caused considerable attack peaks.



LexisNexis® RISK SOLUTIONS

NETWORKED FRAUD CONTINUES TO BE A KEY FEATURE ACROSS ALL GLOBAL REGIONS

Hyperconnected Networks 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.

These fraud networks have been analyzed to expose the number of devices and transaction types involved, as well as the industries and regions impacted.

In this report, this analysis has been extended to:

- Examine the anatomy of key fraud networks regionally.
- Analyze links between fraudulent email addresses and telephone numbers, as well as devices.
- Assign monetary values to the entire fraud network based on known payment transaction amounts.

While these fraud networks are likely to include several different groups of fraudsters, there are some interesting conclusions that can be drawn from the pattern of fraudulent entities. For example:

- It is likely that events linked by a fraudulent device are carried out by the same fraudster or fraud ring.
- However, events linked by fraudulent email addresses and telephone numbers may involve different groups of fraudsters using the same stolen lists of data.

The Digital Identity Network allows organizations to share intelligence related to stolen / synthetic identities and 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.

Interestingly, while devices and email addresses associated with confirmed fraud are both seen operating across regions and industries, telephone numbers associated with confirmed fraud operate almost solely within the same country, and largely across the same industry.

Click here to watch a short video summary of **Networked Fraud Trends.**

EXPOSING THE SIZE AND SCALE OF A FINANCIAL SERVICES FRAUD NETWORK

Sophisticated Fraud Network Targets Organizations Across EMEA

The visualization on the next page shows a fraud network targeting the financial services industry, operating across:

- Several UK banks (see P61 for detailed view).
- Lending organizations in Poland and Latvia (see P62 for detailed view).
- Payments organizations in Austria and Switzerland.

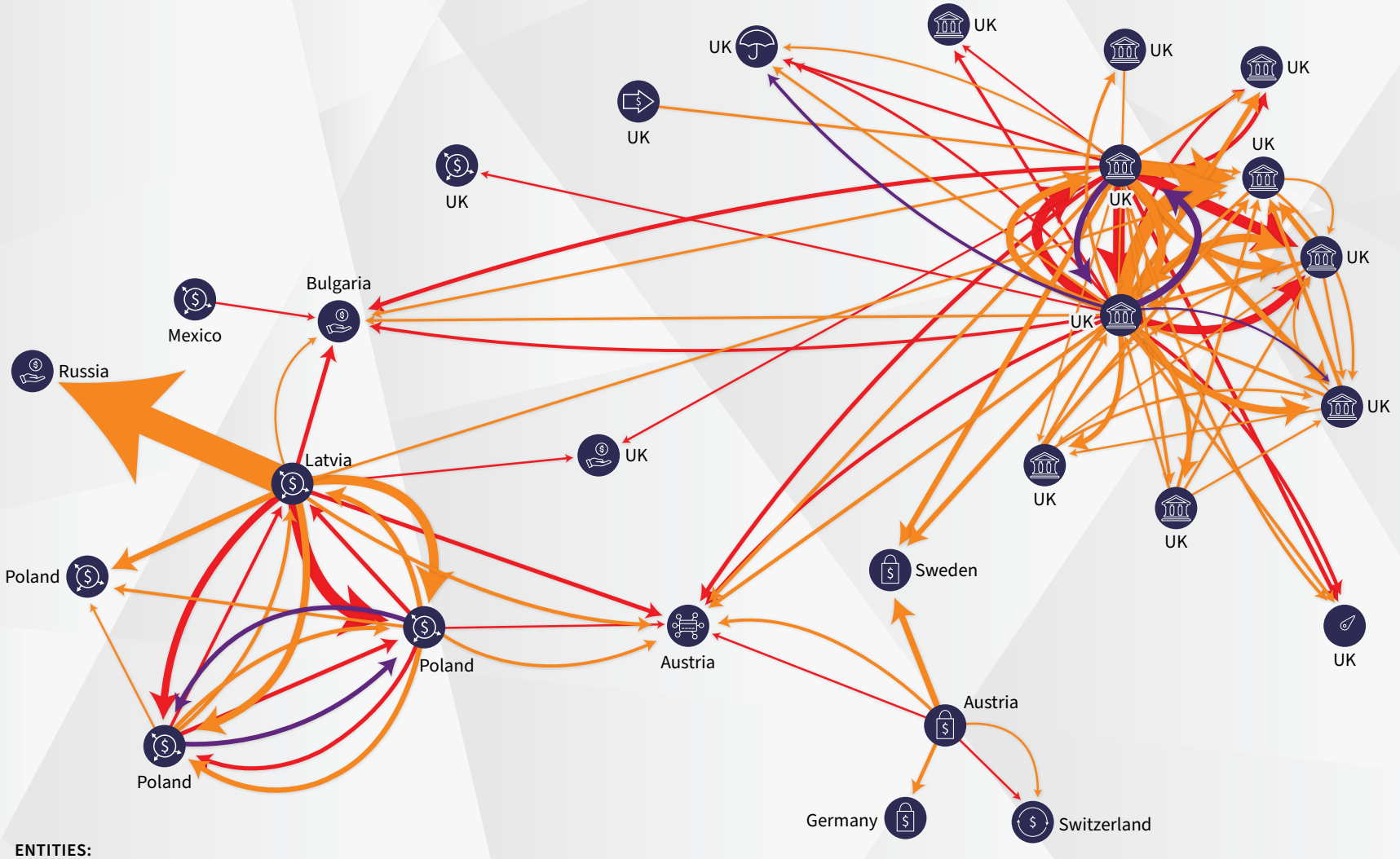
Each arrow illustrates an entity associated with a confirmed fraud event at one organization crossing over to another organization in the Digital Identity Network.

Entities analyzed as part of this network include devices, email addresses and telephone numbers.

Over 37,000 events were associated with a fraudulent entity at the source organization, which was then seen at another organization in the Digital Identity Network. Some events may include more than one type of fraudulent entity.

While devices and email addresses are seen operating across industries and regions, telephone numbers operate predominantly within the same country, and generally across the same industry.

A REGIONAL VIEW



ENTITIES:

- DEVICE
- EMAIL
- TELEPHONE

FINANCIAL SERVICES:

- PAYMENT GATEWAY
- CREDIT SCORING
- BANK
- CARD NETWORK
- MERCHANT PAYMENTS
- LENDING
- COLLECTIONS
- INSURANCE
- REMITTANCE

Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

HUGE E-COMMERCE FRAUD NETWORK OPERATING ACROSS THREE REGIONS

Proliferation of Email Addresses Associated with Fraud Connects Multiple Merchants

The visualization on the next page shows a fraud network targeting the e-commerce industry, operating across:

- Multiple online retailers in the U.S. (see P68 for detailed view).
- A payment gateway in Japan.
- Travel companies and an online marketplace in LATAM.

Each arrow illustrates an entity associated with a confirmed fraud event at one organization crossing over to another organization in the Digital Identity Network.

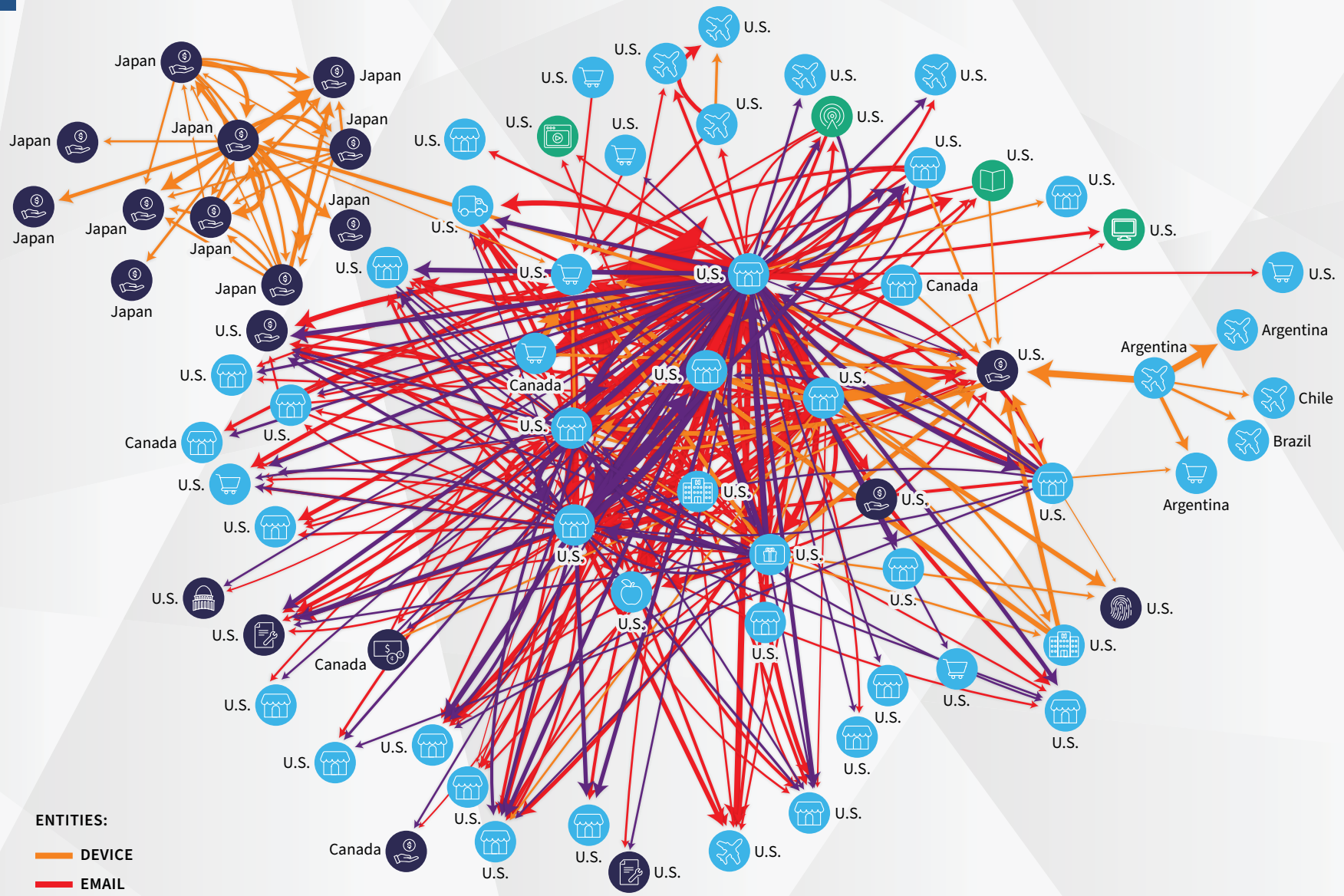
This fraud network sees a higher proliferation of fraudulent events connected through email addresses and telephone numbers, with fewer connections between fraudulent devices, particularly among U.S. merchants.

It's likely that email addresses and telephone numbers that have been compromised as part of a data breach are being used by multiple fraudsters to perpetrate attacks, and hence these show up in thousands of events in the Digital Identity Network.

Over 525,000 events were associated with a fraudulent entity at the source organization, which was then seen at another organization in the Digital Identity Network.

Again, devices and email addresses are seen operating across industries and regions while telephone numbers operate predominantly within the same region (U.S. and Canada) and across similar industries (largely e-commerce).

A REGIONAL VIEW



ENTITIES:

- DEVICE
- EMAIL
- TELEPHONE

FINANCIAL SERVICES:

- PAYMENT GATEWAY
- PERSONAL FINANCE
- GOVERNMENT
- TICKETING
- FRAUD & AUTHENTICATION SERVICES

MEDIA:

- MEDIA STREAMING
- MOBILE OPERATOR
- PUBLISHING
- SOFTWARE

E-COMMERCE:

- MARKETPLACE
- GIFT CARDS
- HEALTHCARE
- RETAILER
- TRAVEL
- FOOD
- LOGISTICS/MAIL DELIVERY

Less than 100 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

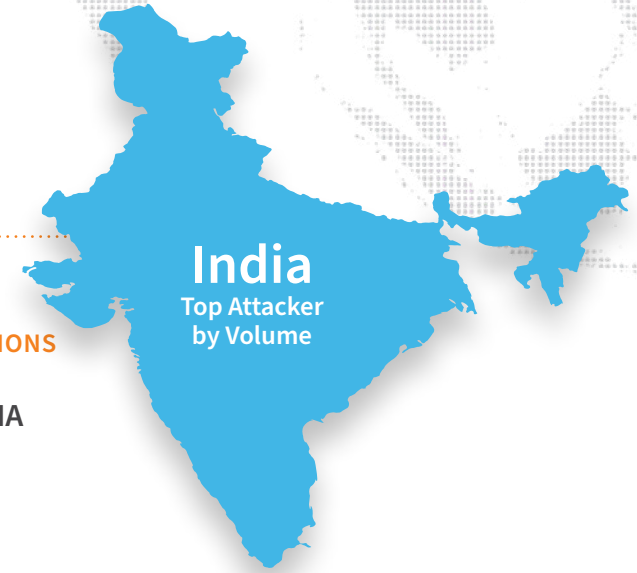
APAC TRANSACTION AND ATTACK PATTERNS

India Tops List of Biggest Regional Attacking Nations

1.4B
Transactions Processed

37M
Human-Initiated Attack Volume

121M
Automated Bot Attack Volume



TOP ATTACK DESTINATIONS FROM INDIA

UK
AUSTRALIA
U.S.
CANADA
INDIA

TRANSACTIONS

Overall
1.4B

Growth YOY
+32% ▲

Transactions Split by **Desktop** / Mobile

43% **57%**

Transactions Split by **Mobile Browser** / App

38% **62%**

ATTACKS

Human-Initiated
37M

Decline YOY
–1% ▼

Automated Bot
121M

Growth YOY
+9% ▲

Attacks Split by **Desktop** / Mobile

49% **51%**

Percentage of attacks coming from mobile devices has increased YOY

+20% ▲

APAC POSITION AGAINST GLOBAL FIGURES

Bot Volume Growth Sits in Contrast to Decline in Human-Initiated Attack Rates

GLOBAL APAC

Although the attack rates in APAC are higher than the global average, they have declined across all channels year-over-year.

The only exception to this trend is the 9% growth in automated bot attacks, although this growth is lower than the global average of 13%.

Japan, India and Australia all make the top ten attackers list for largest global bot originators.

AUSTRALIAN FRAUD NETWORK OPERATES ACROSS ALL 3 CORE INDUSTRIES

Personal Finance Company at the Heart of Complex Fraud Network

Fraud Network by Numbers

25
Organizations in Australia formed a large interconnected fraud network.

The network comprised:

- 2,400 Devices.
- 3,700 Email addresses.
- 1,500 Telephone numbers.

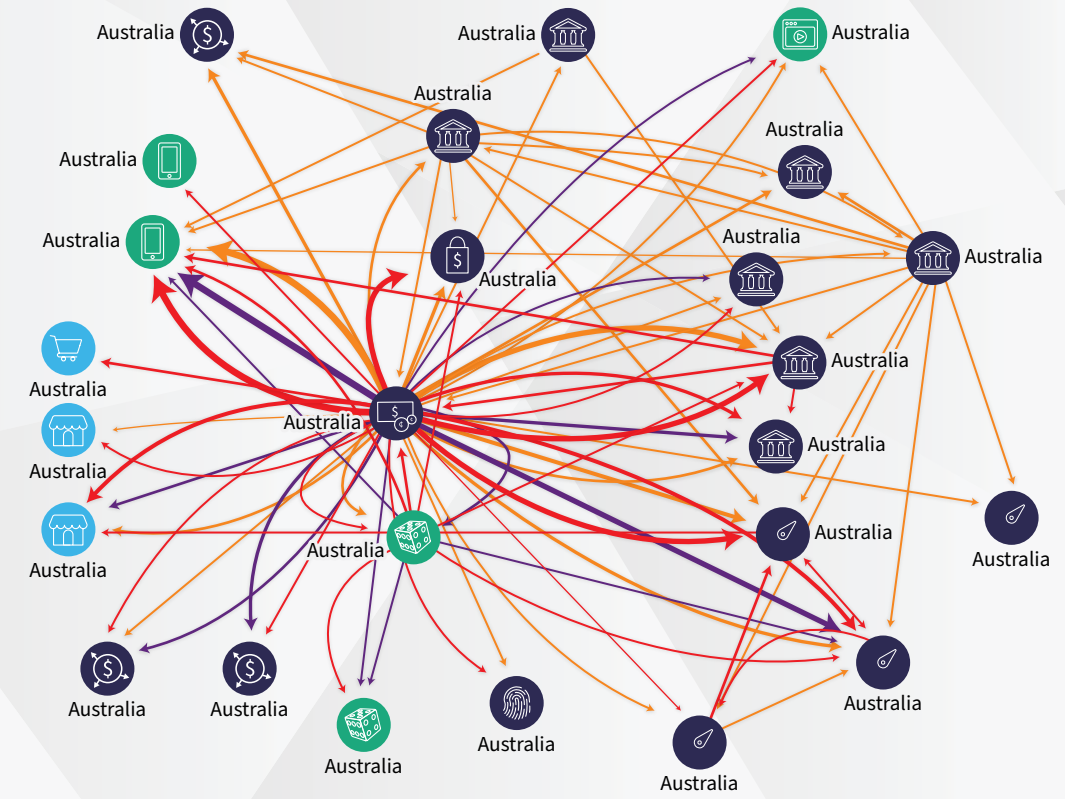
At the source organization:

- 4,950 Events were associated with a fraudulent device
- 7,500 Events were associated with a fraudulent email address
- 3,750 Events were associated with a fraudulent telephone number

Most of these events were new account creations.

Over 8,500
Events at other organizations in the Digital Identity Network were linked to these fraudulent source entities.

At least $800K
Exposed to fraud across entire network.



Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

EMEA TRANSACTION AND ATTACK PATTERNS

Penetration of Mobile Transactions Higher in EMEA than Any Other Region

7.8B
Transactions Processed

71M
Human-Initiated Attack Volume

270M
Automated Bot Attack Volume

TOP ATTACK DESTINATIONS FROM UK

U.S.
UK
CANADA
LATVIA
SWEDEN

TRANSACTIONS

Overall
7.8B

Growth YOY
+31% ▲

Transactions Split by **Desktop** / Mobile

Transactions Split by **Mobile Browser** / App

ATTACKS

Human-Initiated
71M

Decline YOY
-20% ▼

Automated Bot
270M

Growth YOY
+45% ▲

Attacks Split by **Desktop** / Mobile

Percentage of attacks coming from mobile devices has increased YOY

+53% ▲

EMEA POSITION AGAINST GLOBAL FIGURES

Low Overall Attack Rates Punctuated by a Growth in Bot Attack Volume

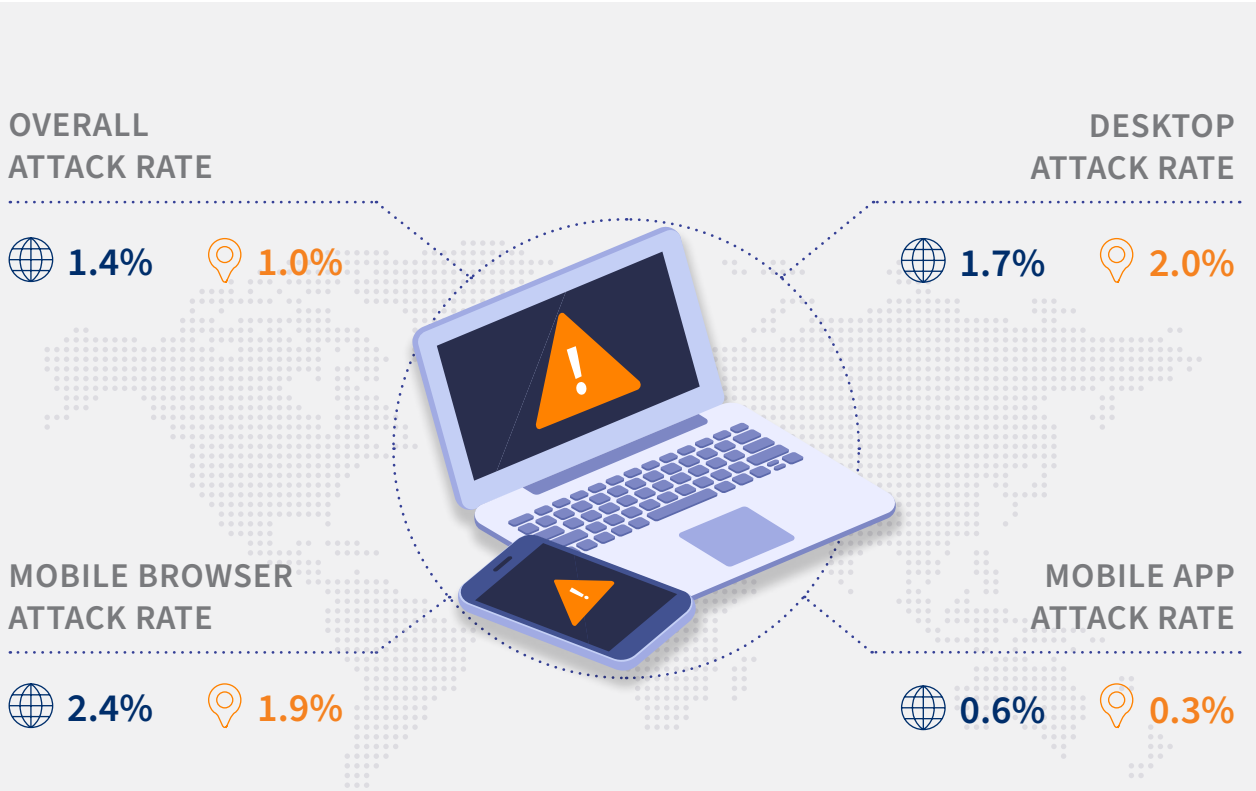
GLOBAL EMEA

The attack rates in EMEA are generally lower than the global average, particularly for mobile app transactions.

This is driven by a high volume of trusted login transactions across relatively mature mobile app propositions.

Notable exceptions in EMEA include:

- Desktop transactions, where the attack rate is higher than the global average.
- Automated bot attack volume, which grew 45% year-over-year.



SPOTLIGHT ON THE ANATOMY OF A UK BANKING FRAUD NETWORK

$17M+ Exposed to Fraud Across 10 Financial Services Organizations

Fraud Network by Numbers

10
UK banks formed part of a larger interconnected fraud network.

The network comprised:

- 7,800 Devices.
- 5,200 Email addresses.
- 1,000 Telephone numbers.

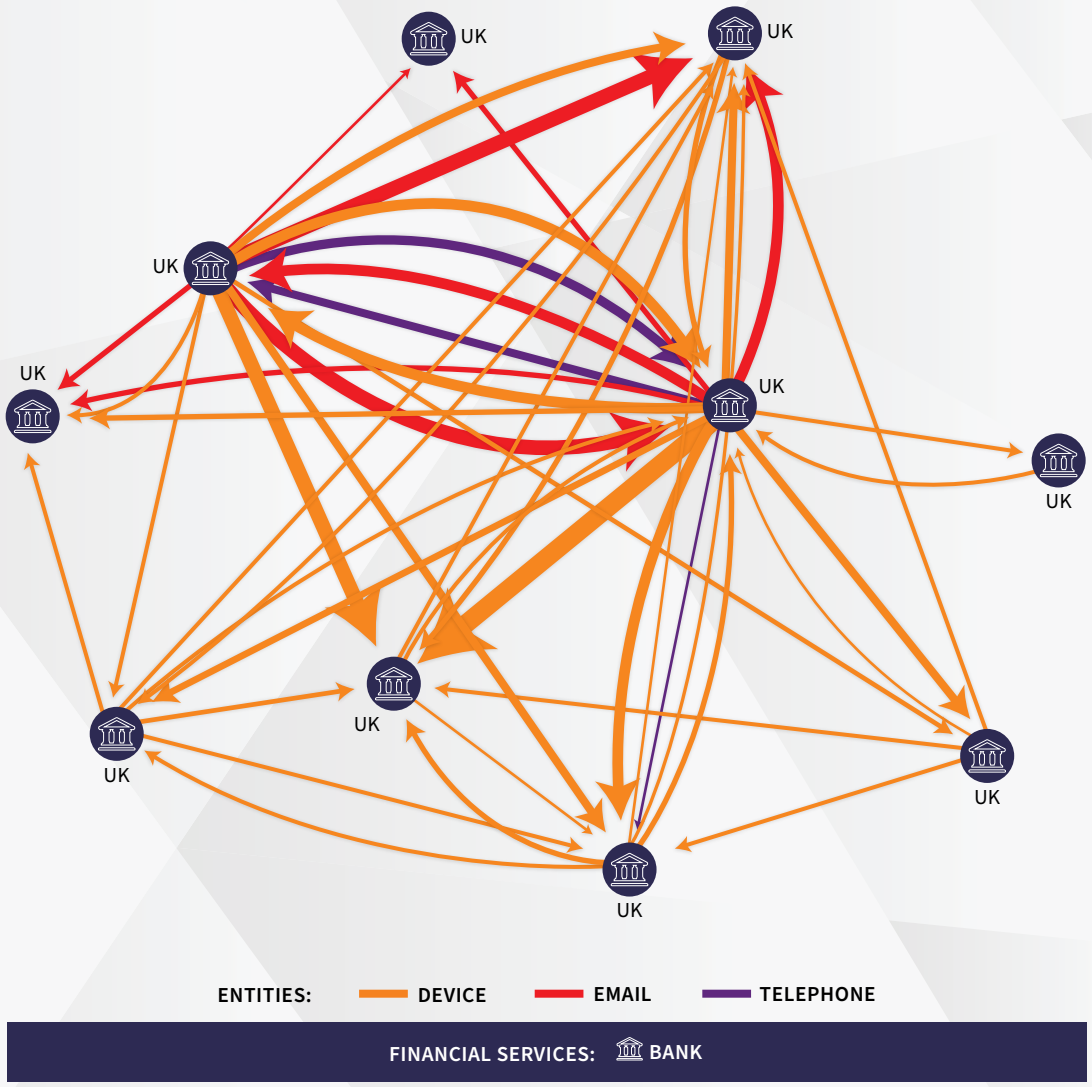
At the source organization:

- 25,300 Events were associated with a fraudulent device
- 8,300 Events were associated with a fraudulent email address
- 1,350 Events were associated with a fraudulent telephone number

Most of these events were logins, but there was also a significant volume of new account creations and payments.

Over 123,000
Events at other organizations in the Digital Identity Network were linked to these fraudulent source entities.

At least $17M
Exposed to fraud across entire network.



Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

SPOTLIGHT ON THE ANATOMY OF AN EASTERN EUROPEAN LENDING FRAUD NETWORK

2,850 Fraudulent New Account Creations Across 4 Regional Lenders

Fraud Network by Numbers

4
Eastern European lending companies formed part of a larger interconnected fraud network.

The network comprised:

- 2,200 Devices.
- 2,900 Email addresses.
- 200 Telephone numbers.

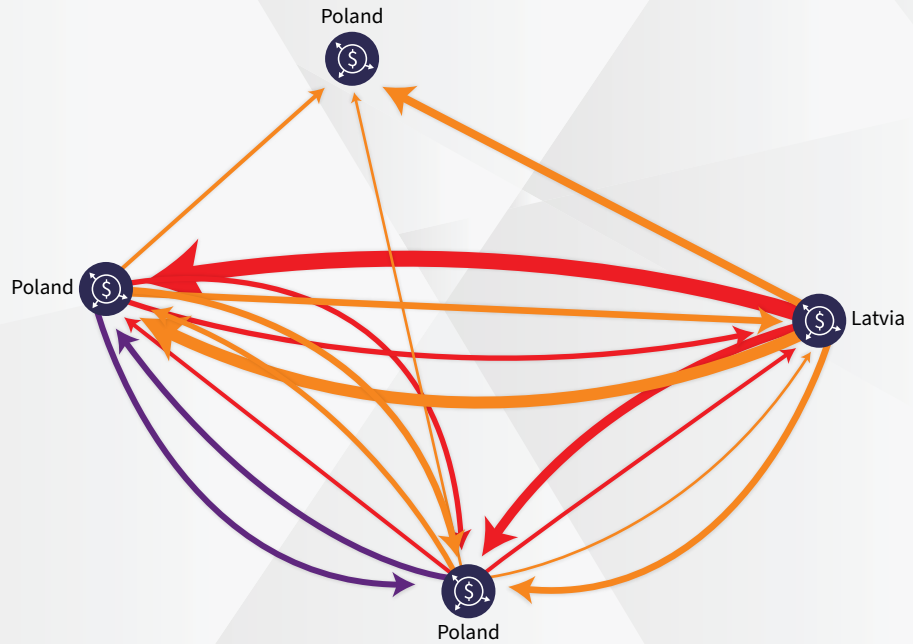
At the source organization:

- 2,300 Events were associated with a fraudulent device
- 3,150 Events were associated with a fraudulent email address
- 370 Events were associated with a fraudulent telephone number

Most of these events were new account creations.

Over 5,500
Events at other organizations in the Digital Identity Network were linked to these source entities.

At least $1.1M
Exposed to fraud across entire network.



Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

LATAM TRANSACTION AND ATTACK PATTERNS

Growth in Human-Initiated and Bot Attack Volume

TOP ATTACK DESTINATIONS FROM BRAZIL

U.S.
ARGENTINA
BRAZIL
CHILE
UK

740M Transactions Processed

39M Human-Initiated Attack Volume

35M Automated Bot Attack Volume

TRANSACTIONS

Overall **740M** — Growth YOY **+63%** ▲

Transactions Split by **Desktop** / Mobile

Transactions Split by **Mobile Browser** / App

ATTACKS

Human-Initiated **39M** — Growth YOY **+23%** ▲

Automated Bot **35M** — Growth YOY **+46%** ▲

Attacks Split by **Desktop** / Mobile

Percentage of attacks coming from mobile devices has increased YOY **+16%** ▲

LATAM POSITION AGAINST GLOBAL FIGURES

Highest Global Attack Rates Compounded by Further Year-Over-Year Growth

GLOBAL LATAM

The attack rates in LATAM are significantly higher than the global average, and are the highest of all global regions.

Attack rates in LATAM appear to be more strongly influenced by the effects of COVID-19 than other regions, with noticeable spikes in attack rates recorded from early March onwards.

LATAM is the only region to experience a growth in attack volume year-over-year. Attacks grew 23%.

LATAM is also the only region to record an overall growth in attack rate for desktop and mobile browser. This growth, however, was only recorded across one period.

LATAM FRAUD NETWORK TARGETS GROUP OF 4 BANKS AND 2 PAYMENT GATEWAYS

Series of Brazilian Financial Institutions See Strong Cross-Organizational Fraud Pattern

Fraud Network by Numbers

6
4 banks and 2 payments gateways in Brazil formed an interconnected fraud network.

The network comprised:

- 1,600 Devices.
- 9,300 Email addresses.
- 500 Telephone numbers.

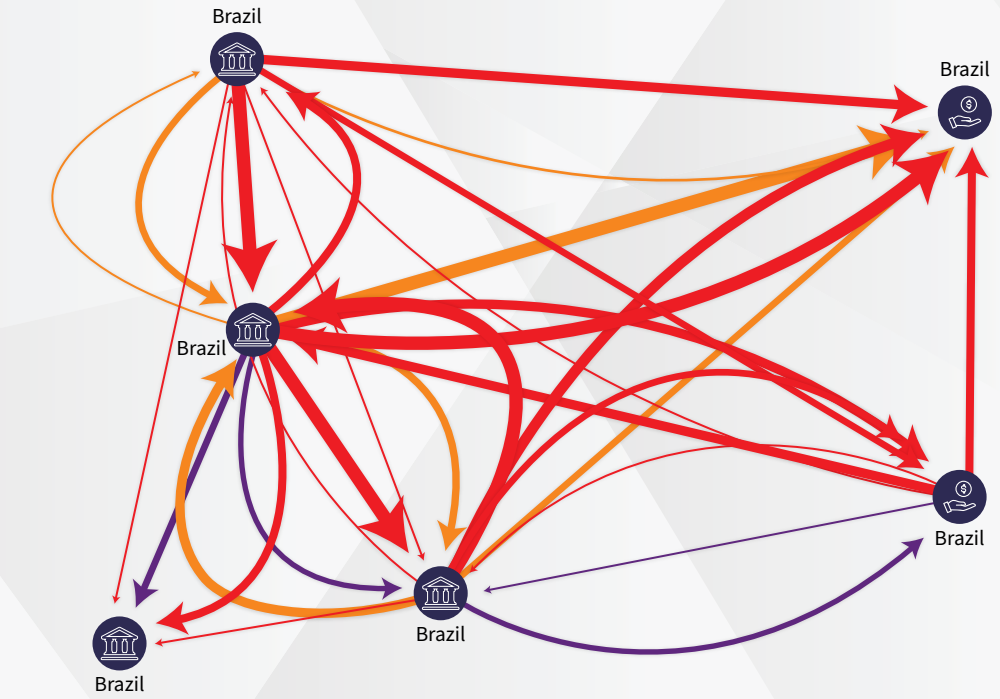
At the source organization:

- 2,850 Events were associated with a fraudulent device
- 15,800 Events were associated with a fraudulent email address
- 880 Events were associated with a fraudulent telephone number

Most of these events were logins, but there was also a significant volume of new account creations and payments.

Over 36,500
Events at other organizations in the Digital Identity Network were linked to these fraudulent source entities.

At least $275K
Exposed to fraud across entire network.



Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

NORTH AMERICA TRANSACTION AND ATTACK PATTERNS

Decline in Human-Initiated and Automated Bot Attack Volume

11.6B
Transactions Processed

109M
Human-Initiated Attack Volume

442M
Automated Bot Attack Volume

TOP ATTACK DESTINATIONS FROM U.S.

U.S.	LATVIA
CANADA	AUSTRALIA
UK	

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

TRANSACTIONS

Overall
11.6B

Growth YOY
+42% ▲

Transactions Split by **Desktop** / Mobile

Transactions Split by **Mobile Browser** / App

ATTACKS

Human-Initiated
109M

Decline YOY
–6% ▼

Automated Bot
442M

Decline YOY
-0.3% ▼

Attacks Split by **Desktop** / Mobile

Percentage of attacks coming from mobile devices has increased YOY

+48% ▲

NORTH AMERICA POSITION AGAINST GLOBAL FIGURES

Low Overall Attack Rates Recorded Across All Use Cases

GLOBAL **NORTH AMERICA**

The U.S. and Canada see lower attack rates across the desktop and mobile browser channels than the global average during this period.

However, the media industry has experienced attack rate growth across all use cases, year-over-year. The financial services industry has experienced attack rate growth across new account creations only.

There is also a strong pattern of networked fraud recorded across the region, highlighted by the large, interconnected e-commerce fraud network targeting multiple retailers in the U.S.

SPOTLIGHT ON THE ANATOMY OF A U.S. E-COMMERCE FRAUD NETWORK

High Volume of Email Addresses Associated with Fraud Shared between Online Retailers and an Online Marketplace

Fraud Network by Numbers

6
5 online retailers and 1 online marketplace in the U.S. formed part of a larger interconnected fraud network.

The network comprised:

- 850 Devices.
- 134,000 Email addresses.
- 61,000 Telephone numbers.

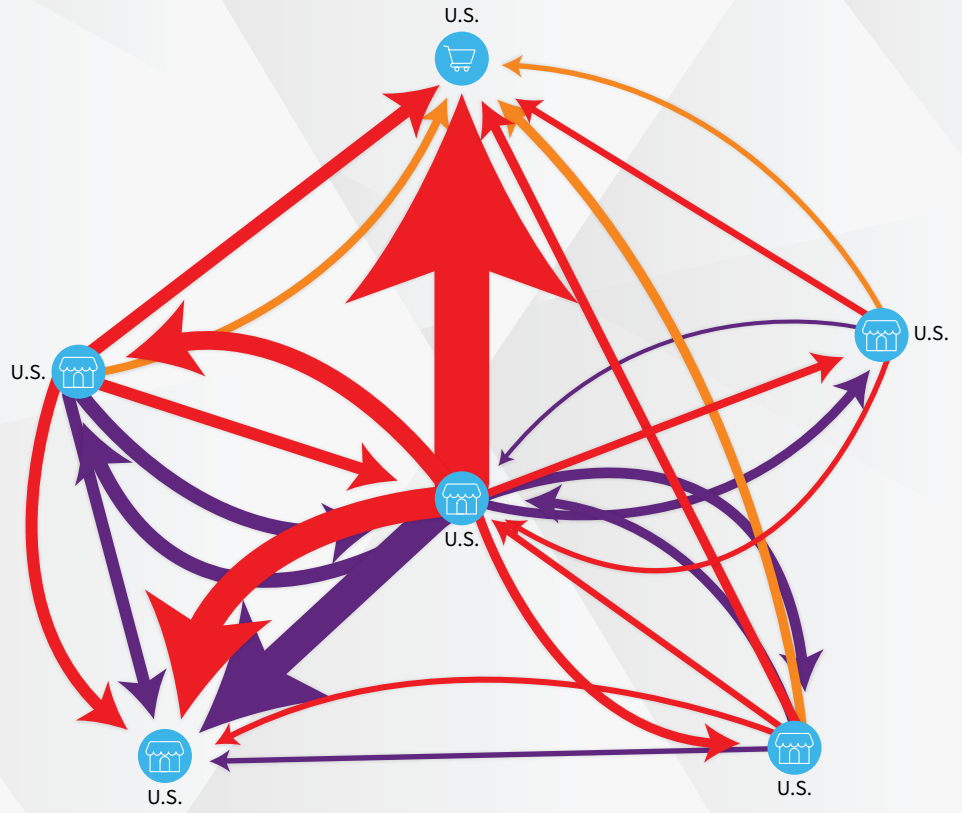
At the source organization:

- 1,230 Events were associated with a fraudulent device
- 200,000 Events were associated with a fraudulent email address
- 105,000 Events were associated with a fraudulent telephone number

All these events were payments.

Over 750,000
Events at other organizations in the Digital Identity Network were linked to these source entities.

At least $27.9M
Exposed to fraud across entire network.



Less than 10 entity overlaps between companies have been removed.

A thicker line denotes a higher volume of fraud.

07

CONCLUSION: A DIGITAL ENVIRONMENT IN FLUX

CONCLUSION AND FUTURE TRENDS

The changing face of cybercrime was clearly evident across regions, industries and businesses January to June 2020. Attacks across the LATAM region grew, media organizations were heavily targeted during the peak of several COVID-19 lockdowns, and many organizations reported attacks of greater intensity or evolving typology.

The financial services industry experienced a growth in automated bot attacks, as well as fraudsters targeting COVID-19-related support packages.

Meanwhile, attacks continued on new account creations that could deliver the promise of lucrative benefits, often using automated bot attacks in higher volume to deliver huge, connected attacks.

As regional lockdowns start to lift and global economies begin their recovery, it will be interesting to see what changes in attack rates the next six months will bring.

Several fraud typologies that have been consistently observed in the Digital Identity Network over time look set to continue. These include:

- Global bot attacks allowing identity testing at scale, providing the opportunity to validate and then monetize stolen credentials.
- Hyperconnected, networked fraud rings tying disparate groups of criminals together to share knowledge and resources for maximum efficacy.

So while the face of cybercrime will continue to re-shape to fit the growing global digital economy, the ability for businesses to reliably recognize good, trusted customers must remain constant. Fraudsters – whether opportunists or highly networked fraud rings – need to be identified and blocked the moment they transact. Knowledge sharing must be as pivotal to global businesses as it is to the cybercriminals that attack them.

Market-leading innovation needs to continue apace to mitigate the complex and changing face of global cybercrime. The following core capabilities should be layered with digital identity intelligence for the next generation of fraud, identity verification and authentication decisioning:

- An integrated decisioning and orchestration layer that can bring together the insight and intelligence of targeted products and solutions.
- An enterprise view of risk across the entire customer journey.
- The integration of complementary data sets and contextualization for enhanced risk decisioning, for example email and behavioral data.
- Personalized authentication journeys tailored to the needs of individual customers, as well as businesses.
- Cross-organizational, cross-industry data sharing via dedicated consortia.
- The development of transactional network analysis, entity linkage and network visualizations.

The Digital Identity Network helps businesses to make near real-time fraud and risk decisions that harness global shared intelligence from thousands of global digital businesses, across millions of daily transactions, and billions of data points. A collaborative network that consistently and reliably identifies online users, even as fraudsters pivot across different attack patterns, industries and global geographies.

08 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.

E-Commerce 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 Creations 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.

Payments 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 LexisNexis® Digital Identity Network.

Attack Percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically, in near real time dependent on individual customer use cases.

Desktop Versus Mobile

Desktop Transactions are transactions that originate from a desktop device such as 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.

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 Digital Identity Network from January-June 2020, 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 January to March 2020, based upon devices, email addresses and telephone numbers recorded as fraudulent in the Digital Identity Network between January and March 2020.
- Monetary exposure calculated on observed payment transactional value at risk January to March 2020, 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.

LexisNexis Emailage

- Intelligence from LexisNexis Emailage March – June 2020, augments analysis from the Digital Identity Network and is included for the first time in this report.
- LexisNexis® Emailage® uses email address metadata, along with customer name, location data, shipping / billing address and phone number, as a basis for transactional risk assessment and digital identity validation.

DATA PROCESSED AND ANALYZED

The overall volume of transactions processed by the Digital Identity Network January – June 2020 was 26.5 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 22.5 billion transactions.

The Cybercrime Report uses these 22.5 billion transactions to calculate overall transaction volumes globally and by region. There are 840K 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 22.5 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 19.2 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

risk.lexisnexis.com/insights-resources/research/cybercrime-report

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: +01 800 062 4989
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.

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