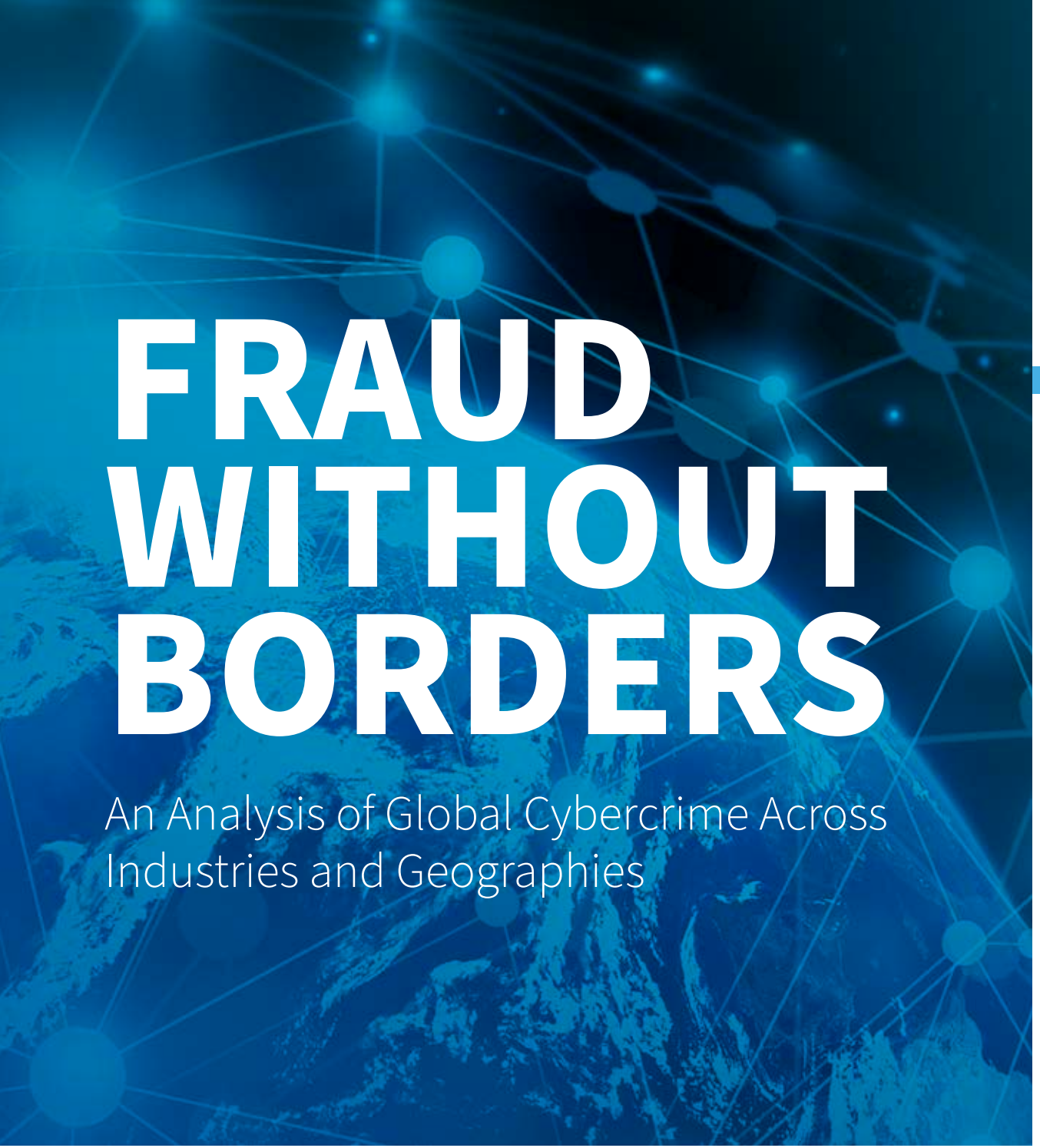

LexisNexis®
RISK SOLUTIONS
FRAUD WITHOUT BORDERS
LexisNexis® Risk Solutions Cybercrime Report
July-December 2019



FRAUD WITHOUT BORDERS

An Analysis of Global Cybercrime Across Industries and Geographies

TABLE OF CONTENTS

LexisNexis® RISK SOLUTIONS

01 INTRODUCTION

Cybercrime: A Global Digital Industry that Permeates Country Borders

CYBERCRIME

A Global Digital Industry that Permeates Country Borders

The global cybercrime industry generates revenues that rival some of the largest economies of the world, with knowledge sharing, services and tools that facilitate global networks of fraud.

In 2014, the Center for Strategic and International Studies (CSIS) estimated that cybercrime cost approximately 0.7% of global income. In 2018 it increased this estimate to 0.8%, or $600 billion a year.* Analysis from the LexisNexis® Digital Identity Network® consolidates the view that cybercrime is a well-organized, global endeavor that enables hyperconnected networks of fraud.

The LexisNexis® Risk Solutions Cybercrime Report has previously tracked the behavior and actions of fraudsters as they operate across multiple organizations within the Digital Identity Network®. This report, however, extends that analysis to look at global fraud networks, analyzing their anatomy by geography, industry and volume. The report combines transaction and attack trends from across the globe with fraud stories from regions, industries and businesses.

In summary, this report analyzes the theme of fraud without borders.

Economic Impact of Cybercrime - No Slowing Down, 2018, McAfee - CSIS

GLOBALLY

Consumers and fraudsters alike are maximizing the opportunities that a global digital economy affords. While consumers enjoy access to goods and services from all over the world, fraudsters harness stolen identity data to launch corresponding global attacks.

Businesses need tools that can identify global fraud while maintaining a low-friction environment for trusted users. Leveraging networks and consortia to share intelligence related to cybercrime and known fraudsters across industries and geographies is more important than ever.

REGIONALLY

Regional nuances in cybercrime reflect the economic, cultural and social differences of each individual country, and can add further context to the analysis of fraud without borders.

Growth economies, for example, are often susceptible to exploitation from fraudsters looking for vulnerabilities in new and emerging processes and platforms. While mature economies may have more layered security defenses, fraudsters can still bypass these with pitch-perfect social engineering scams.

LexisNexis® RISK SOLUTIONS

ANALYZING THE IMPACT OF CYBERCRIME ACROSS GEOGRAPHIES, INDUSTRIES, BUSINESSES AND CONSUMERS

BY INDUSTRY

Cybercriminals often move money across industries, cashing out with a fraudulent payment in financial services, a digital gift card purchase in e-commerce, or a gambling account credit. Likewise, they may use a fraudulent account registration in one industry to make an attack in another industry more successful.

However, despite a common goal, each industry can be susceptible to different types of attacks. Charities, for example, have become targets for small dollar credit card tests. It is these variations and nuances that add further context to the threats that each industry faces as a result of global cybercrime.

AT A BUSINESS LEVEL

Cybercrime can severely hinder the ability for businesses to provide products and services to good, trusted users. Mass bot attacks, for example, sometimes make up 90% of an individual business's daily transaction volume.

Analyzing individual fraud attacks, implementing effective mitigation strategies, and sharing information relating to known fraudsters across businesses facing the same challenges, can help tackle fraudulent networks at their source.

THE IMPACT ON CONSUMERS

Digital consumers who have been victims of fraud are known to change their behavior following an attack. Consumers may reduce their interaction with a service, stop using it altogether, or defect to a competitor, impacting the organization's reputation and bottom line.

Victims of fraud are also affected emotionally and personally. Detecting and blocking attacks before they impact end users can protect individual consumers who ultimately bear the economic, cultural and social turmoil of cybercrime.

LexisNexis® RISK SOLUTIONS

02

FRAUD WITHOUT BORDERS

A GLOBAL VIEW

Global Highlights

Mobile attacks outpace desktop attacks for the first time.

56%
growth in mobile attack rate year over year (YOY).

91M
mobile app registration attempts originate from a global bot attack, heavily influencing the mobile attack rate.

$40M+
at risk from cross-organizational fraud exposure during a one-month period.

73,000+
devices associated with a fraudulent event at one organization were then recorded at another organization within the Digital Identity Network, during a one-month period.

GLOBAL CYBERCRIME IN NUMBERS

Mobile Attacks Outpace Desktop for the First Time

19B
Transactions Processed

401M
Attack Volume

171%
Growth in Mobile App Attack Rate YOY

TRANSACTIONS PROCESSED: 19B

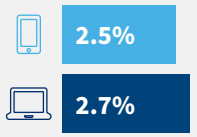
Transactions Split by Mobile / Desktop

Transactions Split by Mobile Browser / App

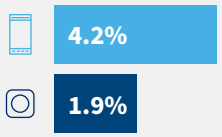
ATTACK TRENDS

Attack Volume | **401M** TOTAL | **264M** | **137M**

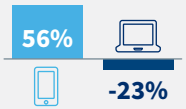
Attack Rates Mobile / Desktop



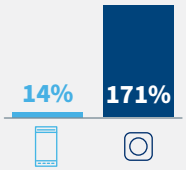
Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop



Attack Rate Growth YOY Browser / App



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

LexisNexis® RISK SOLUTIONS

REPORT HIGHLIGHTS: MOBILE ATTACK RATE GROWS, DESKTOP ATTACK RATE FALLS

Large Bot Attack Targeting Mobile App Account Registrations Impacts Overall Network Trends and Increases Mobile Attack Rate

LexisNexis® RISK SOLUTIONS

MOBILE ATTACKS NOW OUTPACE DESKTOP ATTACKS BY VOLUME, DRIVEN BY A LARGE MOBILE BOT ATTACK.

- While the attack rate of desktop transactions (2.7%), and mobile transactions (2.5%), is almost identical, the mobile attack rate is growing 56% YOY while the desktop attack rate is falling 23% YOY.
- Although this is heavily influenced by a key global bot attack, it nevertheless shows a shift in focus of global cybercrime towards targeting the mobile channel.

MOBILE BROWSER TRANSACTIONS ARE ATTACKED AT A HIGHER RATE, BUT MOBILE APP TRANSACTIONS SEE A BIGGER GROWTH IN ATTACK RATE.

- Mobile browser transactions are attacked at a rate of 4.2%, while mobile app transactions are far safer; attacked at a rate of just 1.9%.
- However, mobile app attacks are growing at a rate of 171% YOY as a result of being targeted by a large global bot, while mobile browser attacks are growing at a steadier rate of 14% YOY.

REPORT HIGHLIGHTS: AUTOMATED BOT TRAFFIC CONTINUES TO IMPACT GLOBAL DIGITAL BUSINESSES

Growth in Bot Traffic Across New Account Creation Transactions

LexisNexis® RISK SOLUTIONS

BOT VOLUMES SEE STRONG GROWTH FROM KEY REGIONS AS FRAUDSTERS USE AUTOMATION TO MAXIMIZE SUCCESS.

- Bot volumes can be very volatile given that one bot attack can represent millions of individual attacks. Analyzing regional growth can give an alternative view of how automated bot traffic is targeting specific industries and geographies.
- The Digital Identity Network has recorded strong growth in bot attacks from Canada, Germany, France, India and Brazil, despite the fact that the global bot volume has fallen YOY.
- Bots from Canada, France and Germany were all targeting the same group of organizations, which were mainly financial services and media. Although these bots were predominantly focused on account takeovers, the number of account creation bot attacks increased globally during the second half of 2019.
- An example of this growth can be seen in the financial services industry, where account creation transactions were targeted by the same bot coming from Brazil, India and Thailand, indicating how fraudsters are using multiple locations to launch targeted attacks.

A GLOBAL VIEW

REPORT HIGHLIGHTS: GROWING THREAT OF NETWORKED CYBERCRIME

Digital Identities Associated with Confirmed Fraud Recorded Across More than One Organization

LexisNexis® RISK SOLUTIONS

STRONG PATTERN OF CROSS-ORGANIZATIONAL, CROSS-INDUSTRY FRAUD RECORDED BY THE DIGITAL IDENTITY NETWORK.

Throughout 2019, the Digital Identity Network has tracked numerous examples of fraudsters working across the global banking network, e-commerce merchants, media organizations, fintech providers and credit reference agencies.

The strongest correlation of fraud was across organizations in the same industry. However, correlations were also present across organizations in disparate industries.

In this report, this analysis has been further extended to:

- Map out the detailed anatomy of global fraud networks to better understand global, regional and industry connections.
- Detail the size and scope of cross-organizational fraud by analyzing the number of devices and transaction types involved.
- Assign monetary values to the fraud networks based on known transaction values.

Several key insights from the analysis of these global networks have emerged:

In just one month, over 73,000 devices were associated with fraud at more than one organization within the Digital Identity Network.

Key fraud networks analyzed for this report all involved organizations from more than one region, confirming the global nature of networked fraud.

All fraud networks analyzed also involved organizations from more than one industry, illustrating how cybercriminals launder money across the global digital economy for maximum financial gain.

Many of the fraud networks had so many interlinking devices and transactions, that they were too complex to illustrate in one clear view.

The largest individual network analyzed spanned six countries, included all three core industries (financial services, e-commerce and media), with $12.5M exposed to fraud in one month.

LexisNexis® RISK SOLUTIONS

THE ANATOMY OF GLOBAL FRAUD NETWORKS

Fraudsters Target Organizations Across Country Borders

This report introduces new analysis of fraud networks operating globally across regions, industries and organizations. Several individual fraud networks are analyzed in detail throughout the report using the methodology below.

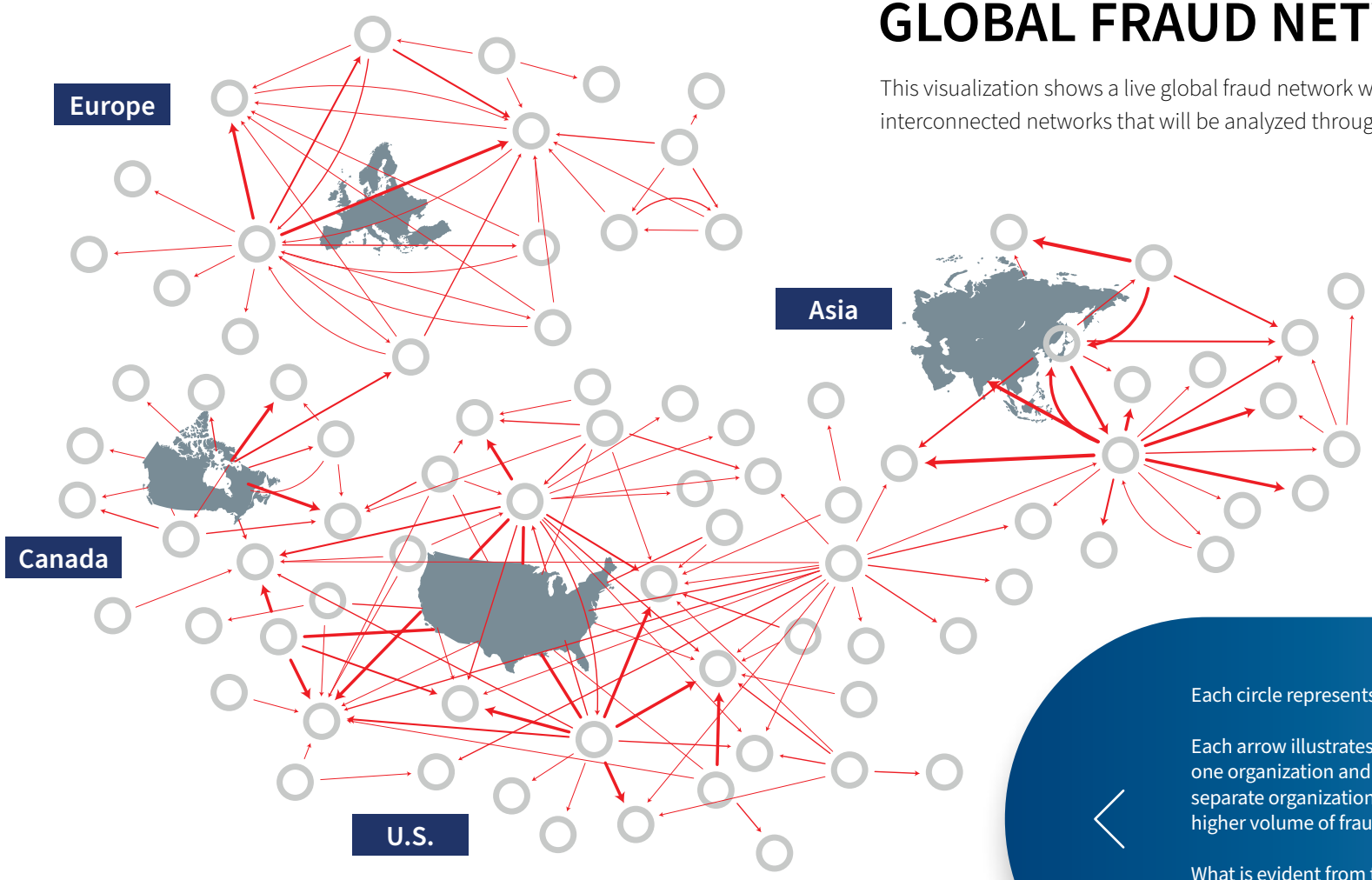
Methodology

- Analysis conducted on confirmed fraud events across global digital businesses within the Digital Identity Network.
- Identification of all devices associated with fraud at first organization.
- These devices were then linked to transactions at other organizations.
- Fraudulent devices from the first organization that are then seen at subsequent organizations are represented with an arrow.

LexisNexis® RISK SOLUTIONS

GLOBAL FRAUD NETWORKS

This visualization shows a live global fraud network with several smaller interconnected networks that will be analyzed throughout the report.



Each circle represents one organization.

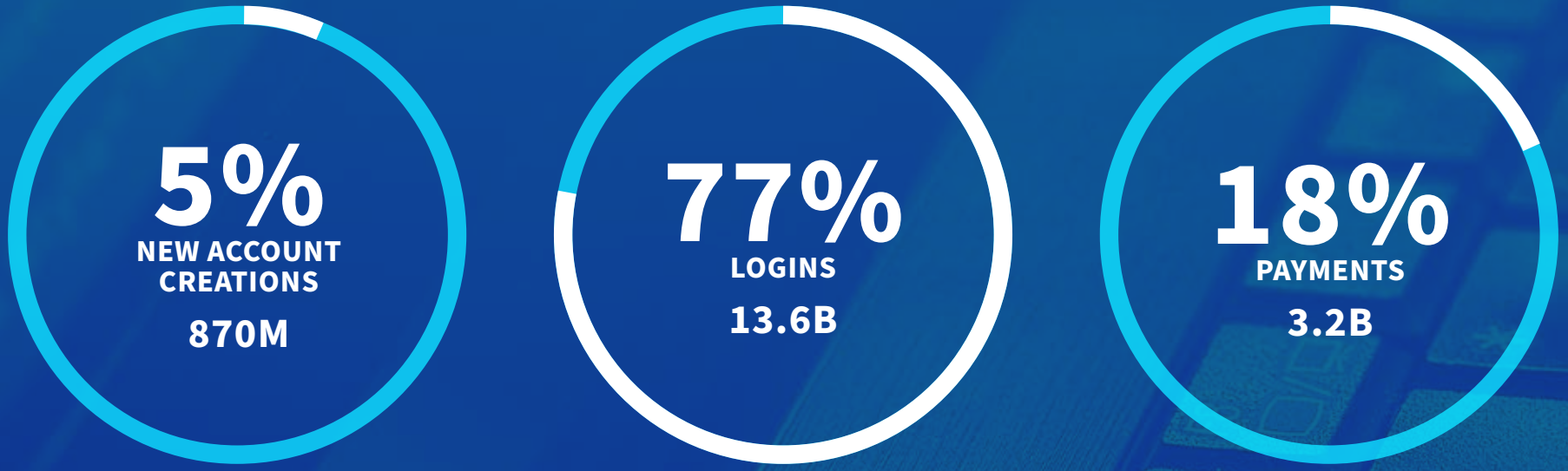
Each arrow illustrates fraud originating from one organization and crossing over to another separate organization. A thicker line denotes a higher volume of fraud.

What is evident from this visualization is that hyperconnected fraud networks exist locally, regionally and globally and offer valuable insight into the wider fraud ecosystem.

LexisNexis® RISK SOLUTIONS

TRACKING GLOBAL FRAUD ACROSS THE ONLINE CUSTOMER JOURNEY

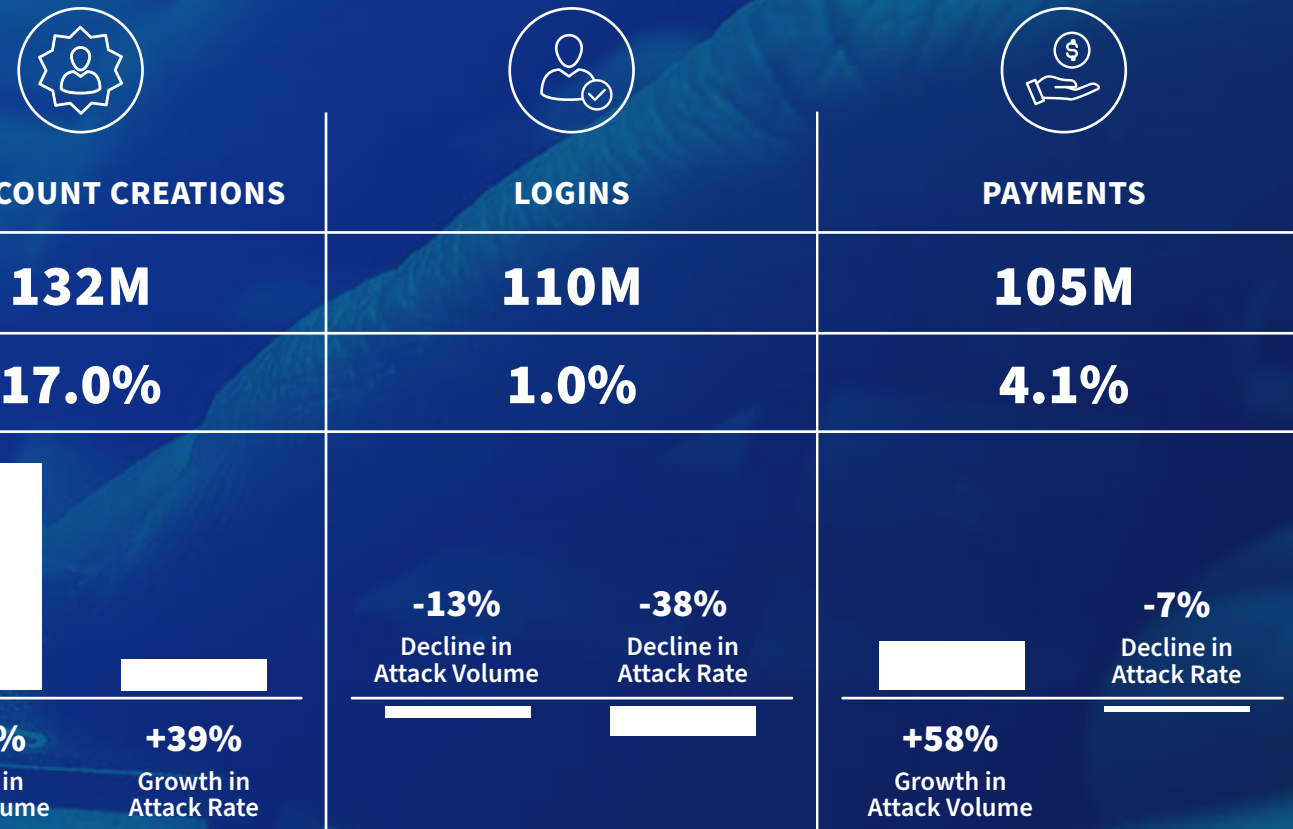
VOLUME OF TRANSACTIONS*



** Transaction and attack volumes listed as "other" e.g. change of details, internal transfers, have been omitted from this analysis, but are part of the total volume of transactions analyzed in the report*

ATTACK VOLUME GROWS IN NEW ACCOUNT ORIGINATIONS AND PAYMENTS

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK VOLUME	132M	110M	105M
ATTACK RATE	17.0%	1.0%	4.1%
ATTACK RATE GROWTH / DECLINE YOY	+293% Growth in Attack Volume +39% Growth in Attack Rate	-13% Decline in Attack Volume -38% Decline in Attack Rate	+58% Growth in Attack Volume -7% Decline in Attack Rate
	New account creations are most at risk during this period, as a result of a large global bot attack targeting new mobile app registrations.	Logins are the safest transactions as a proportion of overall transaction volume; repeat transactions help businesses to build trust levels of good, returning users.	The growth in payment attacks is slightly less than the growth in payment transaction volume, indicating a stable risk environment despite a moderate attack rate.



** Attack volume and attack rate are calculated using a subset of the total transaction volume, where outliers, and attacks on some transaction types such as change of details and internal transfers are removed.*

A GLOBAL VIEW

IDENTITY ABUSE INDEX

Tracking the Impact of Breached Credentials on Global Digital Businesses

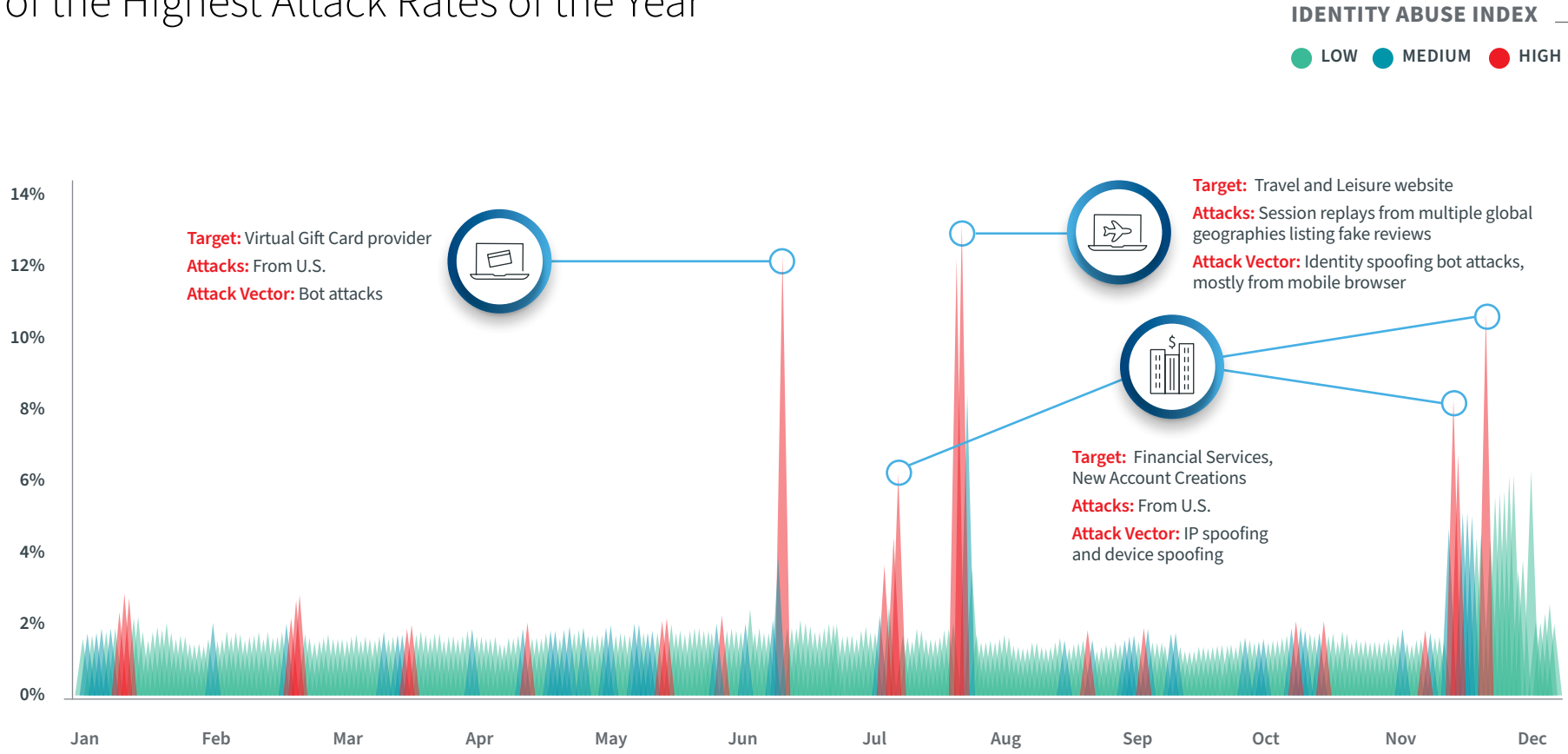
The LexisNexis Risk Solutions Identity Abuse Index shows the percentage of attacks per day, across the entire Digital Identity Network, providing a clear representation of large attack peaks throughout 2019.

These attacks are often driven by automated bots mass testing identity credentials or creating fake reviews. These bots rely on a fresh and ready supply of stolen identity data, harvested from global data breaches experienced by virtually all industries. New account creations are the most “at-risk” use case.

LexisNexis® RISK SOLUTIONS

MASS AUTOMATED BOTS CAUSE ATTACK PEAKS ACROSS ALL INDUSTRIES

The Second Half of 2019 Recorded Several of the Highest Attack Rates of the Year



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

LexisNexis® RISK SOLUTIONS

TOP 10 GLOBAL ATTACKERS BY COUNTRY OF ORIGIN

LATAM Solidifies its Position on the Cybercrime World Stage

The Network's largest attack volumes have consistently originated from the economic powerhouses of North America and Europe, with strong digital transaction volumes recorded in these key geographies.

However, emerging economies continue to play an ever-growing role in cybercrime as breached identity data disseminates globally.

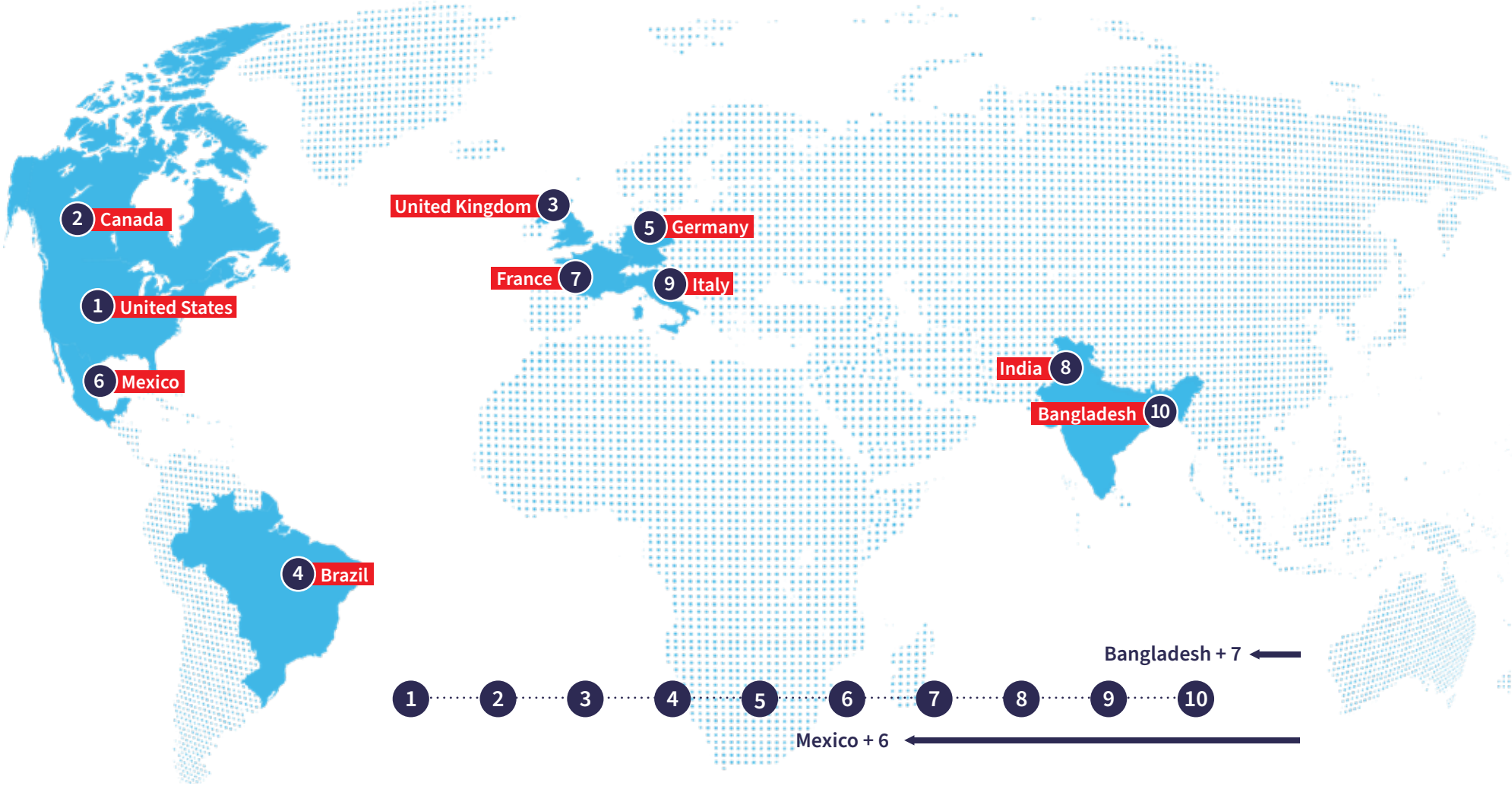
In comparison to the same period last year:

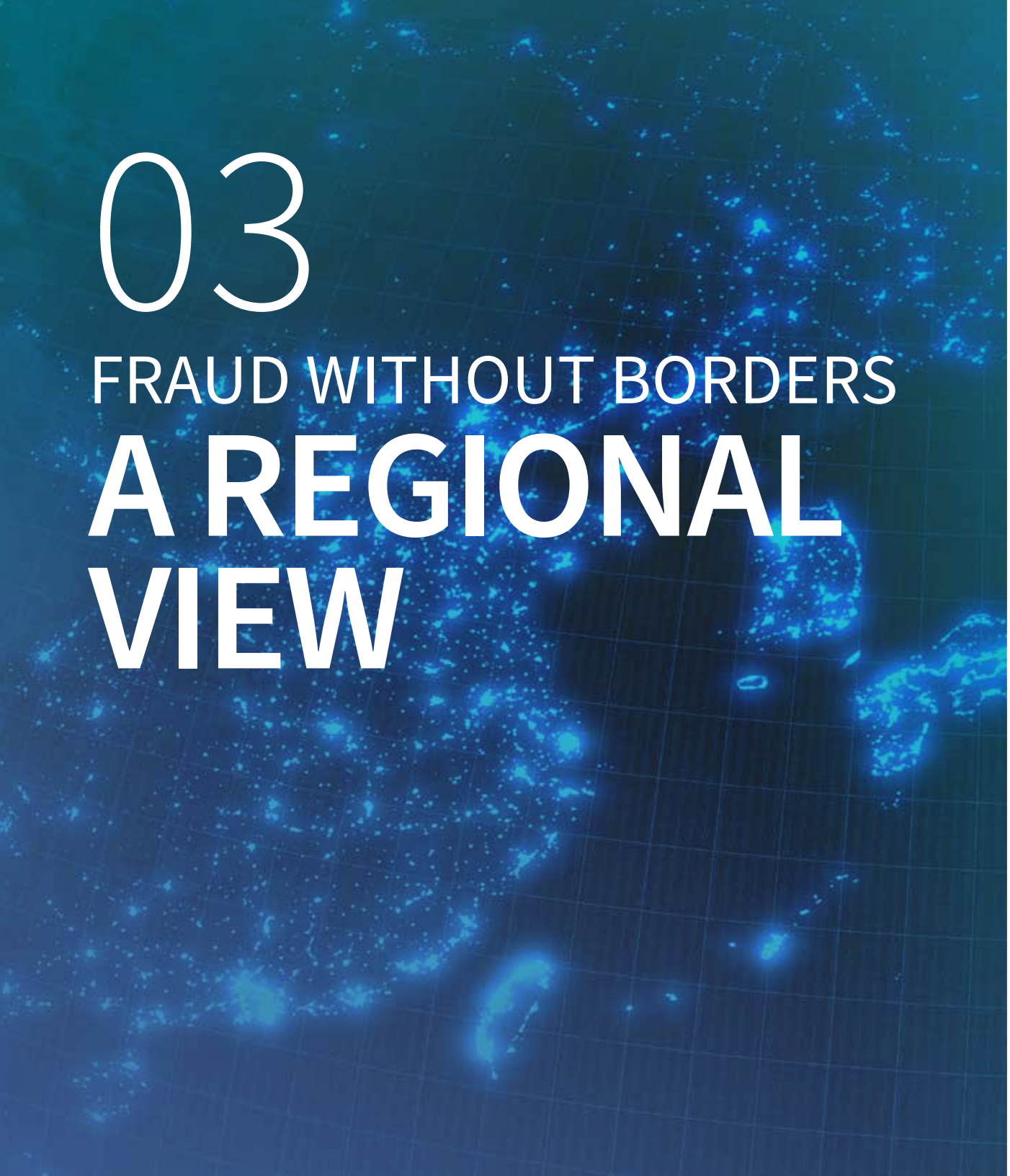
- Brazil has remained the fourth biggest attacking nation.
- Mexico has climbed six places in the top attackers list.
- Bangladesh has climbed seven places in the top attackers list.

Albania, Bosnia and Herzegovina, Algeria, Tunisia and Serbia all have high attack rates as a percentage of total transactions, despite the fact they don't make the list of top attacking nations by volume.

SPREAD OF TOP ATTACKERS CONFIRMS CYBERCRIME IS A TRULY GLOBAL INDUSTRY

All Key Regions Represented in the Top Attackers List





03

FRAUD WITHOUT BORDERS

A REGIONAL VIEW

Regional Highlights

APAC

Lowest penetration of mobile transactions, with lower tolerance for risk.

EMEA

Highest penetration of mobile transactions, but growth in mobile app attacks.

LATAM

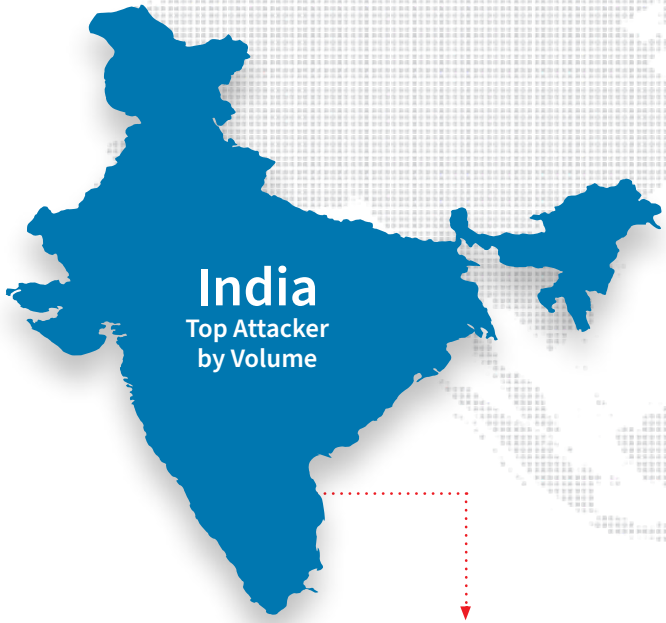
Higher than average attack rates across all desktop and mobile transactions.

NORTH AMERICA

Lowest overall attack rate on desktop transactions, with growth in mobile app attacks.

APAC CYBERCRIME IN NUMBERS

India Tops List of Biggest Regional Attacking Nations



1.3B
Transactions Processed

57M
Attack Volume

116%
Growth in Mobile App Attack Rate YOY

TOP ATTACK DESTINATIONS FROM INDIA

U.S.
AUSTRALIA
UK
CANADA
INDIA

TRANSACTIONS PROCESSED: 1.3B

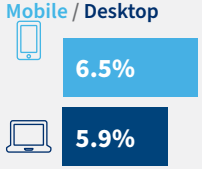
Transactions Split by Mobile / Desktop

Transactions Split by Mobile Browser / App

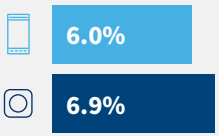
ATTACK TRENDS

Attack Volume | **57M** TOTAL | **32M** | **25M**

Attack Rates Mobile / Desktop

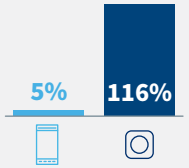


Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop

Attack Rate Growth YOY Browser / App



LexisNexis® RISK SOLUTIONS

APAC'S POSITION AGAINST GLOBAL FIGURES

Less Mobile Region with Lower Tolerance for Risk

	GLOBAL	APAC
MOBILE TRANSACTION VOLUME	67%	58%
MOBILE ATTACK VOLUME	66%	56%
MOBILE ATTACK RATE	2.5%	6.5%
MOBILE BROWSER ATTACK RATE	4.2%	6.0%
MOBILE APP ATTACK RATE	1.9%	6.9%
DESKTOP ATTACK RATE	2.7%	5.9%

- The APAC region sees a higher overall attack rate than globally, driven by strong attack volumes from India.
- The Digital Identity Network also saw large regional bot volumes targeting global financial services organizations.
- Despite the high attack rate, financial services organizations in the region generally experience lower fraud. This is in part due to higher rates of step-up and enhanced authentication strategies; both an accepted part of the overall customer journey.

Due to the relative scale of the network, including large organizations in the most digitally active regions, the absolute attack rates of each of the global regions can vary, and disproportionately influence the performance metrics of regions that experience smaller transaction volumes.

A REGIONAL VIEW

APAC EXPERIENCES STRONG BOT ACTIVITY

Automated Attacks Target Financial Services New Account Creations

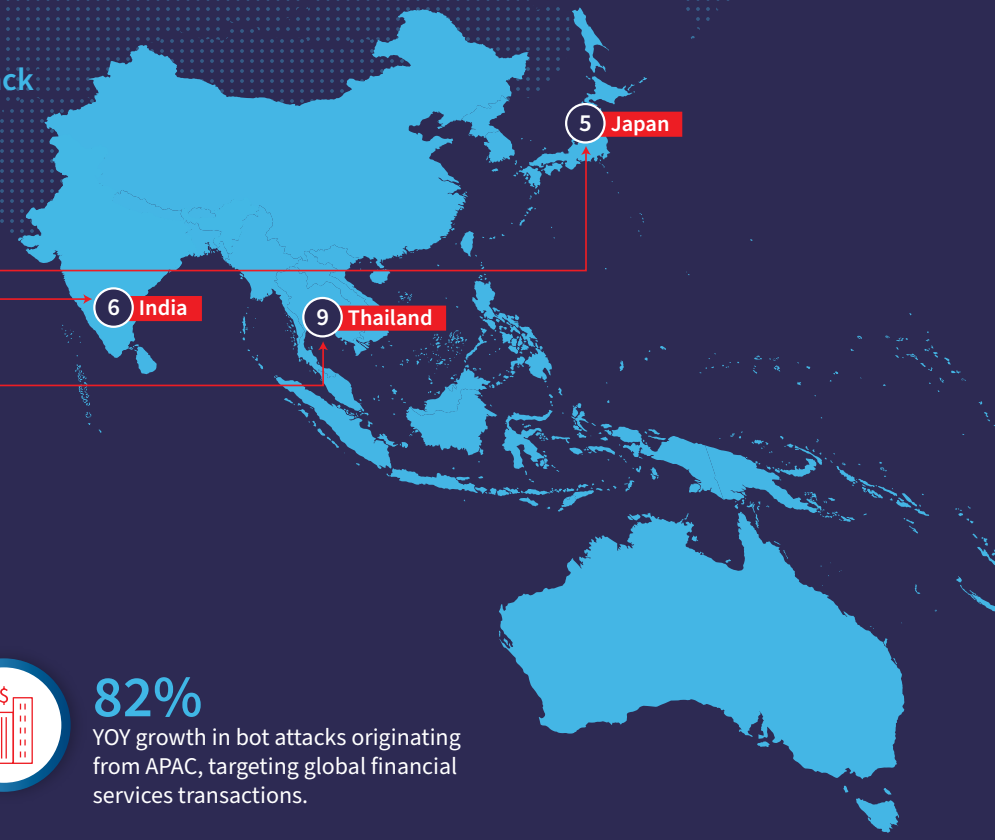
While some of this bot traffic comes from "good" bots, namely aggregators accessing financial services organizations, a high percentage of attacks are maliciously targeting logins and new account creations using stolen or spoofed identity credentials.

Bots originate from the most highly developed of APAC countries, through to emerging and growth economies. This shows the widespread dissemination and use of breached identity data.

Bot traffic in the APAC region is predominantly targeting financial services institutions, specifically new account creation processes.

Top 10 Bot Attack Originators

1. U.S.
2. UK
3. Canada
4. Germany
5. Japan
6. India
7. Brazil
8. France
9. Thailand
10. Russia



82%

YOY growth in bot attacks originating from APAC, targeting global financial services transactions.

APAC PLAYS KEY ROLE IN GLOBAL FRAUD NETWORKS

Cross-Organizational, Cross-Region Network Includes Several APAC Businesses

Mirroring bot patterns that operate across country borders, several APAC financial services organizations have been recorded in a fraud network that crosses over into EMEA and North America.

This fraud network saw confirmed fraud events at banks in Singapore, Hong Kong and India. This fraud also extended to banks in the United Arab Emirates, a travel company in United Arab Emirates, and a Healthcare Provider in the U.S., extending the geographical footprint of fraud from the region.

An Indian financial services organization sits at the center of this fraud network. This bank saw devices associated with confirmed fraud cross-over to five other organizations within the Digital Identity Network.

The Digital Identity Network saw more attacks from India than any other country in the APAC region during the second half of 2019.

LexisNexis® RISK SOLUTIONS

APAC AND MIDDLE EAST-FOCUSED FRAUD NETWORK

Cross-Over Between Financial Services and E-Commerce Organizations

Anatomy of Fraud Network

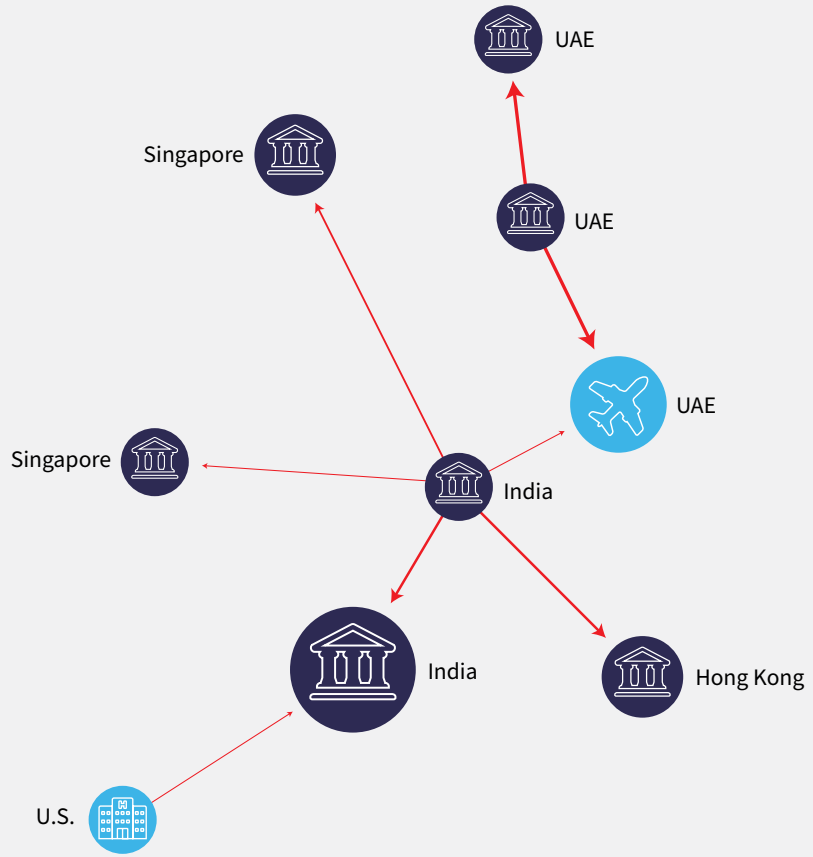
200
Devices associated with fraud, cross over with more than one organization.

900
Cross-organizational events are login transactions.

150
Cross-organizational events are payment transactions.

$11M+
Exposure to fraud at original organization.

$350k
Exposure to fraud at cross-over organizations in one-month period.



A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud. Less than 10 device overlaps between companies have been removed.

LexisNexis® RISK SOLUTIONS

EMEA CYBERCRIME IN NUMBERS

High Mobile Penetration Offers New Opportunity to Fraudsters in the Region

7B
Transactions Processed

126M
Attack Volume

233%
Growth in Mobile App Attack Rate YOY

TOP ATTACK DESTINATIONS FROM UK

U.S.
UK
CANADA
IRELAND
AUSTRALIA

TRANSACTIONS PROCESSED: 7B

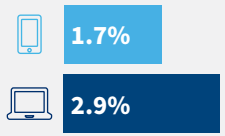
Transactions Split by Mobile / Desktop

Transactions Split by Mobile Browser / App

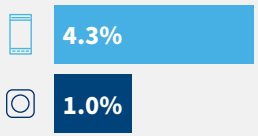
ATTACK TRENDS

Attack Volume | **126M** TOTAL | **81M** | **45M**

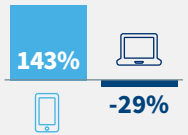
Attack Rates Mobile / Desktop



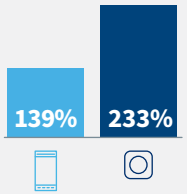
Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop



Attack Rate Growth YOY Browser / App



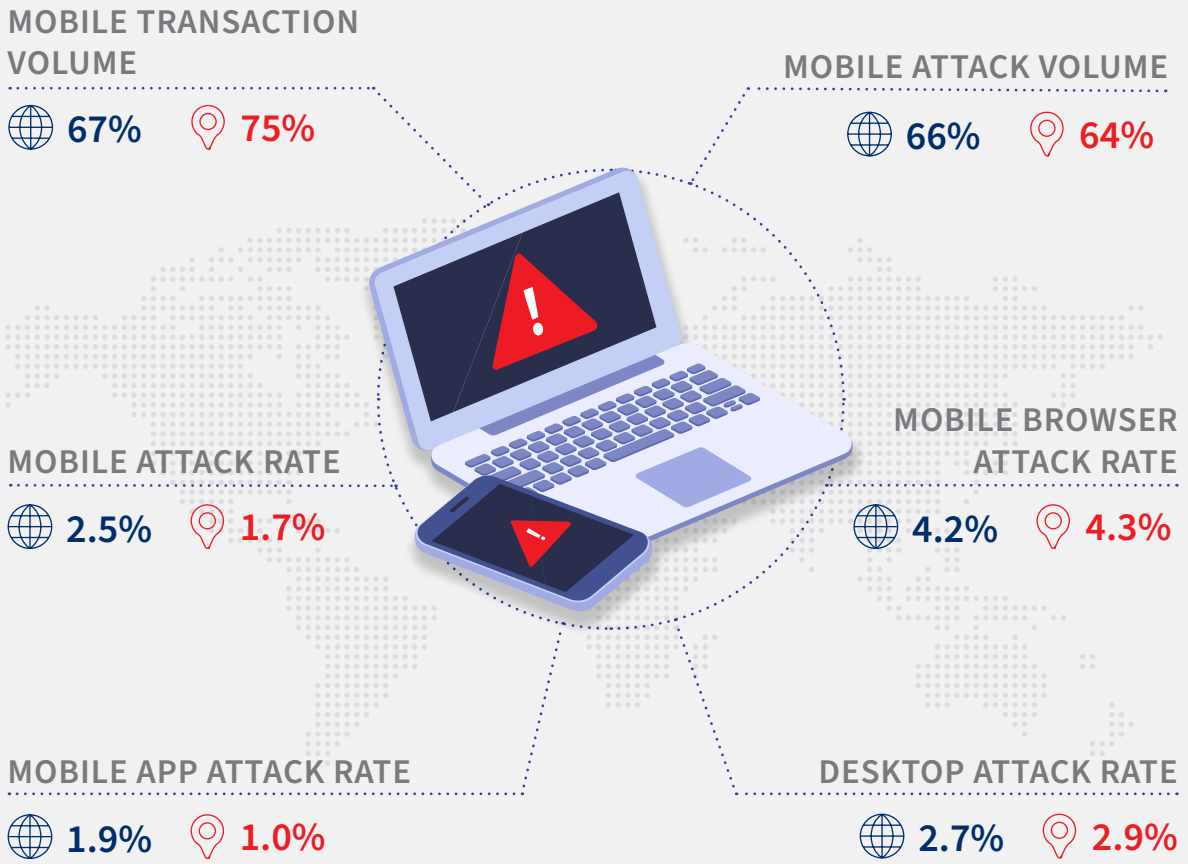
LexisNexis® RISK SOLUTIONS

EMEA'S POSITION AGAINST GLOBAL FIGURES

Mature Digital Economy Drives High Mobile Penetration, But Attacks on Mobile App Transactions Growing

GLOBAL **EMEA**

- EMEA sees the highest penetration of mobile transactions of all global regions, driven by a mature digital economy.
- Financial services and media see the highest penetration of mobile transactions at 83% and 65% respectively, while e-commerce mobile penetration is just 44%.
- The strongest growth in mobile penetration is seen in:
  - E-commerce logins – 40% YOY.
  - Financial services new account creations – 50% YOY.
- While overall attack rates are consistent with global figures, the mobile app attack rate is lower than the global average. However, there are strong pockets of growth in attack rates YOY, particularly in mobile app new account creations across all industries.



LexisNexis® RISK SOLUTIONS

GLOBAL FRAUD NETWORK CENTERED AROUND UK BANKS

Huge Fraud Network Points to Global Mule Activity in Financial Services

While financial services organizations in EMEA see low overall attack rates (largely due to the high volume of login transactions from good returning customers), mule accounts remain one of the biggest fraud challenges for UK banks.

Global mule networks form the primary way to siphon proceeds of crime through the banking ecosystem, as they attempt to avoid detection and capture.

Fraudsters are creating their own mule account base by:

- Registering new accounts with stolen / spoofed credentials.
- Persuading individuals (either knowingly or unwittingly) to set-up, compromise or allow access to bank accounts to exit stolen funds.

Proceeds of crime can filter through multiple mule accounts and across country borders in near real time, facilitated by faster payments initiatives both in the UK and worldwide.

The Digital Identity Network has detected a fraud network that appears to bear the hallmarks of a mule network, encompassing several UK banks and lenders, financial services institutions in the U.S., Canada and France, as well as retailers and media companies that span all regions.

This huge global network highlights the truly global footprint of fraudulent mule networks and the requirement for global data sharing that can be facilitated in near real time.

UK BANKING FRAUD NETWORK, CROSSING OVER TO CANADA, U.S. AND FRANCE

Network Operates Across 6 Countries and All 3 Core Industries

Anatomy of Fraud Network

2,200
Devices associated with fraud, cross over with more than one organization.

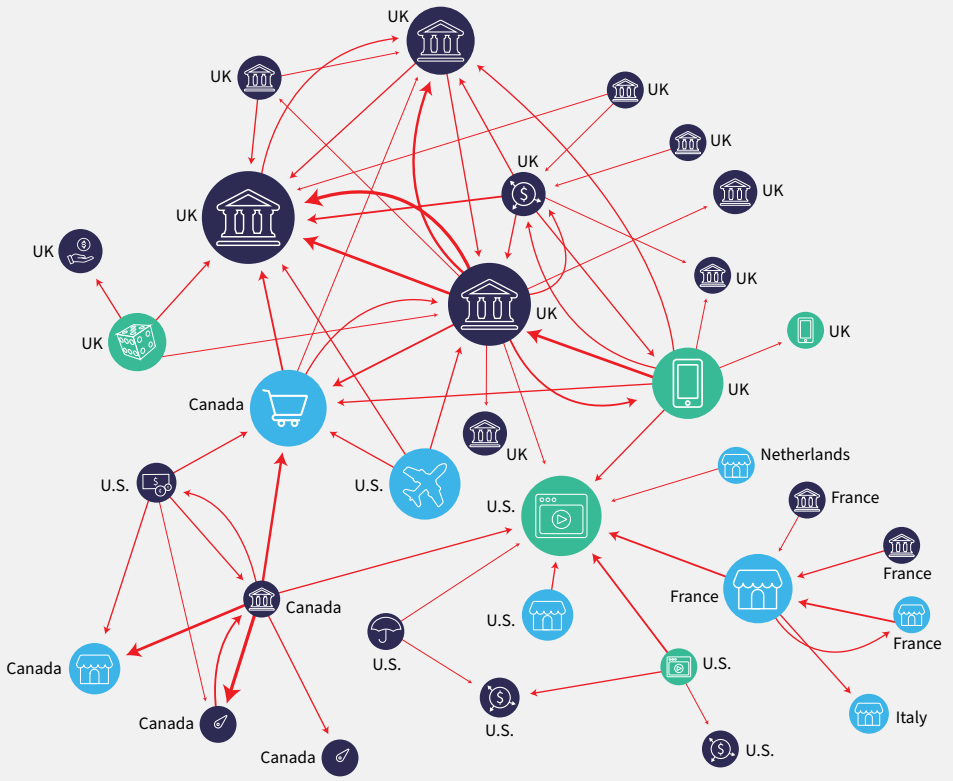
2,000
Cross-organizational events are new account creations.

13,500
Cross-organizational events are login transactions.

2,500
Cross-organizational events are payment transactions.

$9M
Exposure to fraud at original organization.

$3.5M
Exposure to fraud at cross-over organizations in one-month period.



FINANCIAL SERVICES:	PERSONAL FINANCE	BANK	CREDIT SCORING
	PAYMENT GATEWAY	LENDING	INSURANCE
MEDIA:	MEDIA STREAMING	TELCO	GAMING/GAMBLING
E-COMMERCE:	MARKET PLACE	RETAILER	TRAVEL

A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud. Less than 10 device overlaps between companies have been removed.

LexisNexis® RISK SOLUTIONS

LATAM CYBERCRIME IN NUMBERS

Digital Transformation Makes Region Susceptible to High Attack Rates

724M
Transactions Processed

45M
Attack Volume

97%
Growth in Mobile App Attack Rate YOY

TOP ATTACK DESTINATIONS FROM BRAZIL

U.S.
ARGENTINA
BRAZIL
UK
LATVIA

TRANSACTIONS PROCESSED: 724M

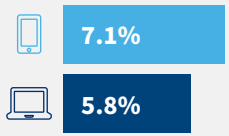
Transactions Split by Mobile / Desktop

Transactions Split by Mobile Browser / App

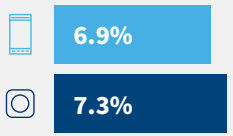
ATTACK TRENDS

Attack Volume | **45M** TOTAL | **33M** | **12M**

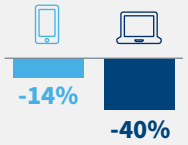
Attack Rates Mobile / Desktop



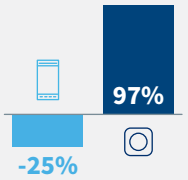
Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop



Attack Rate Growth YOY Browser / App



LexisNexis® RISK SOLUTIONS

LATAM'S POSITION AGAINST GLOBAL FIGURES

Digitally Agile Region with Strong Mobile Transaction and Attack Growth

	GLOBAL	LATAM
MOBILE TRANSACTION VOLUME	67%	69%
MOBILE ATTACK VOLUME	66%	73%
MOBILE ATTACK RATE	2.5%	7.1%
MOBILE BROWSER ATTACK RATE	4.2%	6.9%
MOBILE APP ATTACK RATE	1.9%	7.3%
DESKTOP ATTACK RATE	2.7%	5.8%

- LATAM experiences high overall attack rates and bucks the global trend with a very high mobile app attack rate, heavily influenced by a large global bot attack on mobile app registrations.
- This is particularly prevalent in financial services and media, where the attack rate is more than one in every five new mobile app registrations, and has grown significantly YOY.
- This trend suggests that fraudsters may be targeting mobile banking / media streaming apps that are new to market. The Digital Identity Network recorded large attacks at a social networking site, as well as an increase in attacks at a financial services organization during the second half of 2019.

KEY FRAUD NETWORK IN LATAM SHOWS LINKS WITH NORTH AMERICA

Complex E-Commerce Scam Operates Across Multiple Organizations and Geographies

The Digital Identity Network has identified an example of a complex and interconnected fraud network involving a series of e-commerce merchants in the LATAM region, including a large online marketplace, and several travel providers.

This fraud also has connections to payment gateways in both LATAM and the U.S., as well as a money remittance provider in the U.S. It is likely that these payment providers are unwittingly processing fraudulent transactions from the e-commerce merchants via stolen credit card data.

An online gift card merchant forms part of this fraud network, suggesting the fraudsters may be using digital gift cards as a way of cashing out or monetizing stolen credit cards, or otherwise taking over good user accounts to access gift card balances.

LexisNexis® RISK SOLUTIONS

LATAM FRAUD NETWORK CENTERED AROUND ARGENTINA

Cross-Over Between E-Commerce and Financial Services Organizations

Anatomy of Fraud Network

1,100
Devices associated with fraud, cross over with more than one organization.

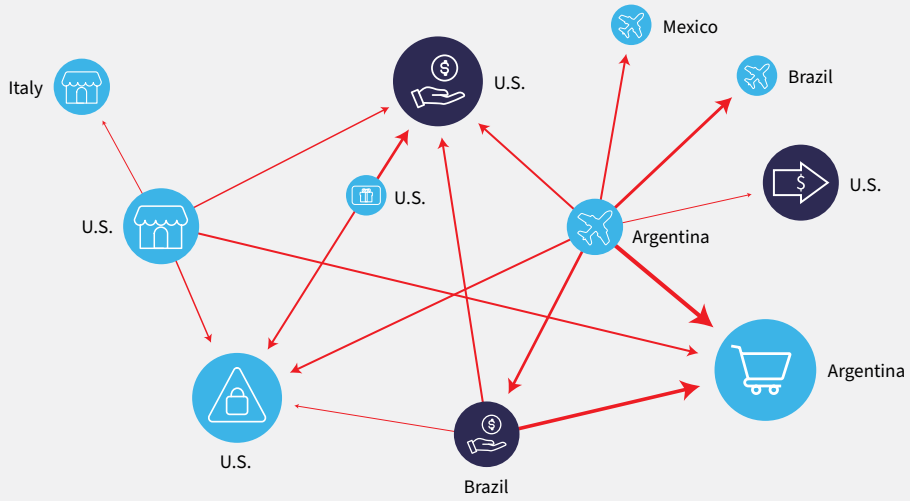
9
Cross-organizational events are new account creations.

175
Cross-organizational events are login transactions.

6,000
Cross-organizational events are payment transactions.

$18,000
Exposure to fraud at original organization.

$13,000
Exposure to fraud at cross-over organizations in one-month period.



FINANCIAL SERVICES:	PAYMENT GATEWAY	REMITTANCE	
E-COMMERCE:	MARKET PLACE	RETAILER	TRAVEL
	FRAUD PREVENTION	GIFT CARDS	

A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud. Less than 10 device overlaps between companies have been removed.

LexisNexis® RISK SOLUTIONS

NORTH AMERICA CYBERCRIME IN NUMBERS

Decline in Desktop and Mobile Browser Attack Rate, Growth in Mobile App Attack Rate

9.1B
Transactions Processed

167M
Attack Volume

138%
Growth in Mobile App Attack Rate YOY

TOP ATTACK DESTINATIONS FROM U.S.

U.S.
CANADA
UK
AUSTRALIA
ARGENTINA

TRANSACTIONS PROCESSED: 9.1B

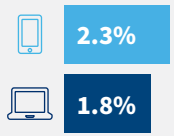
Transactions Split by Mobile / Desktop

Transactions Split by Mobile Browser / App

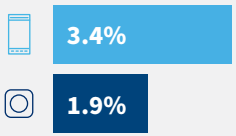
ATTACK TRENDS

Attack Volume | **167M** TOTAL | **115M** | **52M**

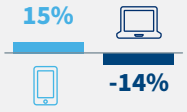
Attack Rates Mobile / Desktop



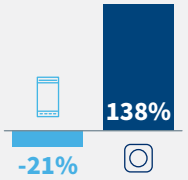
Attack Rates Mobile Browser / App



Attack Rate Growth YOY Mobile / Desktop



Attack Rate Growth YOY Browser / App



LexisNexis® RISK SOLUTIONS

NORTH AMERICA'S POSITION AGAINST GLOBAL FIGURES

Desktop Transactions Attacked at a Lower Rate than Globally, Despite Growth in New Account Creation Attacks

	GLOBAL	NORTH AMERICA
MOBILE TRANSACTION VOLUME	67%	63%
MOBILE ATTACK VOLUME	66%	69%
MOBILE ATTACK RATE	2.5%	2.3%
MOBILE BROWSER ATTACK RATE	4.2%	3.4%
MOBILE APP ATTACK RATE	1.9%	1.9%
DESKTOP ATTACK RATE	2.7%	1.8%

- North America sees the lowest desktop attack rate of all regions, with the only growth in attack rates seen on new account creation transactions, particularly in financial services.
- Mobile attack rates are consistent with global figures:
  - There was a growth in mobile app attacks recorded across all industries YOY.
  - Only the media industry saw a growth in mobile browser attacks YOY.

THE ANATOMY OF TWO NORTH AMERICAN FRAUD NETWORKS

Analysis of Fraudulent Events in the Digital Identity Network Finds Confirmed Examples of Cross-Organizational Fraud Rings. These are Further Substantiated via Customer Intelligence.

LexisNexis® RISK SOLUTIONS

Key Highlights:

Identification of two fraud networks operating across multiple organizations in North America.

Fraudulent behavior identified across these organizations by the Digital Identity Network and linked to one device.

Intelligence from this device is then cross-referenced to internal e-commerce customer database which identifies a wider fraud network.

Key risk indicators and intelligence from this wider fraud network subsequently linked to other organizations within the Digital Identity Network.

LexisNexis® RISK SOLUTIONS

1. IDENTITY SPOOFING FRAUD WITH CASH-OUT AT E-COMMERCE MERCHANT

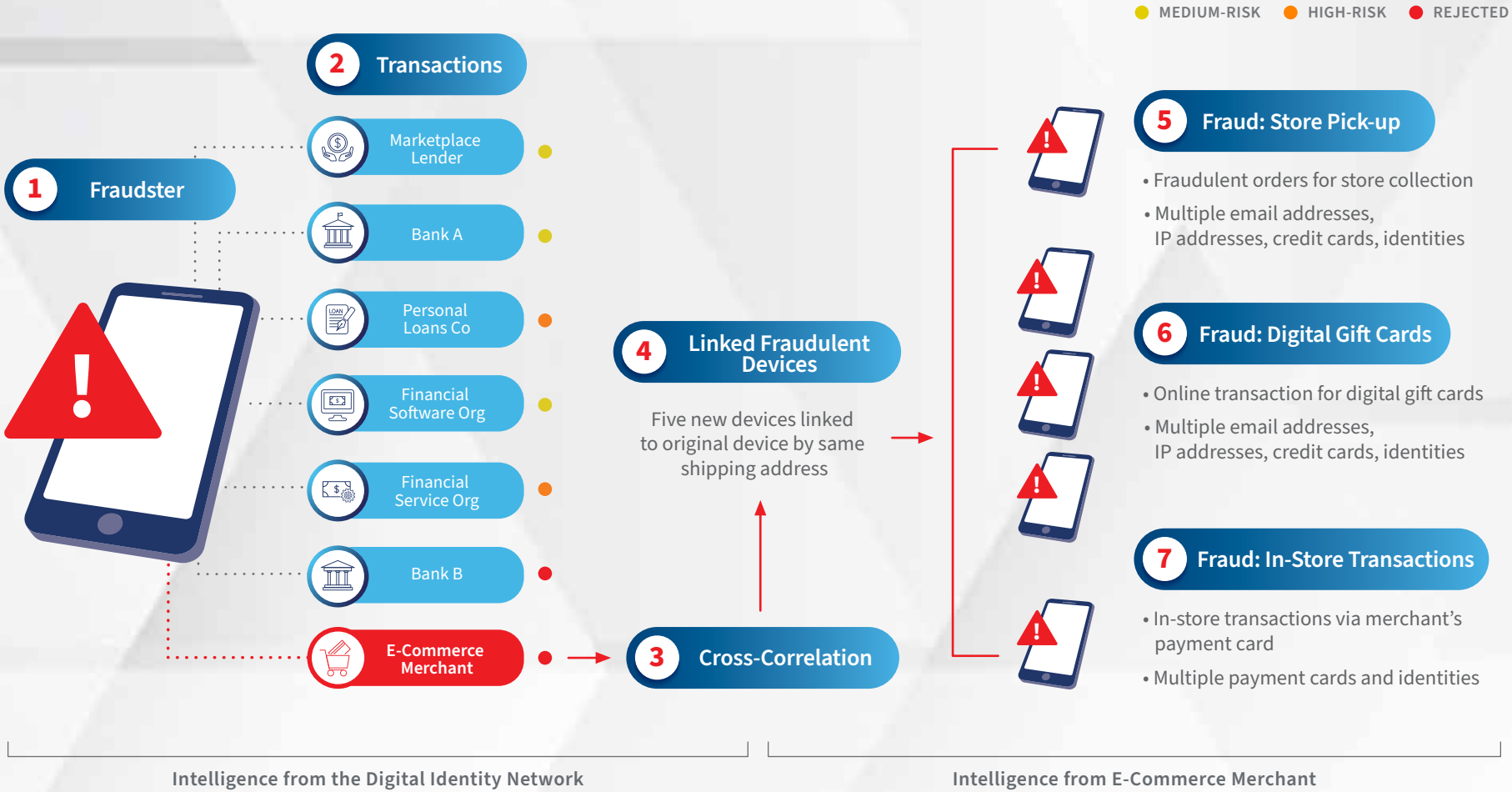
Initial Fraud Linked to Spider Web of Fraud Typologies at Merchant

LexisNexis® RISK SOLUTIONS

A REGIONAL VIEW:
ANATOMY OF FRAUD NETWORKS

LexisNexis® RISK SOLUTIONS

E-COMMERCE MERCHANT UNCOVERS NETWORKED FRAUD RING USING INTELLIGENCE FROM THE DIGITAL IDENTITY NETWORK



LexisNexis® RISK SOLUTIONS

DECONSTRUCTING THE ANATOMY OF IDENTITY SPOOFING FRAUD RING

1 Fraudster

A fraudster was tracked carrying out a series of transactions, many of which were high-risk and fraudulent, across multiple organizations within the Digital Identity Network.

- *These transactions were linked to one device, despite the fact the fraudster was attempting to bypass device fingerprinting.*

2 Transactions

The fraudster tried to open accounts at lenders and banks, as well as perform several logins and payments across multiple organizations.

- *This could indicate a potential identity spoofing fraud, with the fraudster testing multiple identity credentials to open accounts, takeover good user accounts or monetize stolen credit cards.*
- *Each organization assessed the transactions according to their own policies and tolerance for risk. However several transactions were marked as confirmed fraud, including a payment transaction at the e-commerce merchant.*

3 Cross-Correlation

The e-commerce merchant took the device intelligence from this fraudulent pattern of transactions and cross-correlated it to its own network.

4 Linked Fraudulent Devices

The e-commerce merchant linked the original fraudulent device to five other devices via one unique shipping address. These additional five devices were also linked to further confirmed fraud attempts at the e-commerce merchant, creating a larger, complex fraud network.

5 Fraud: Store Pick-Up

One of these devices was associated with a fraud network using store pick-up, with multiple email addresses, IP addresses, credit cards and identities.

6 Fraud: Digital Gift Cards

Three of these devices were associated with digital gift card fraud on the merchant's website, and were also associated with multiple email addresses, IP addresses and credit cards.

7 Fraud: In-Store Transactions

The final device was associated with a series of fraudulent payments in-store using the merchant's own payment card method. This fraud also logged multiple payment cards and identities.

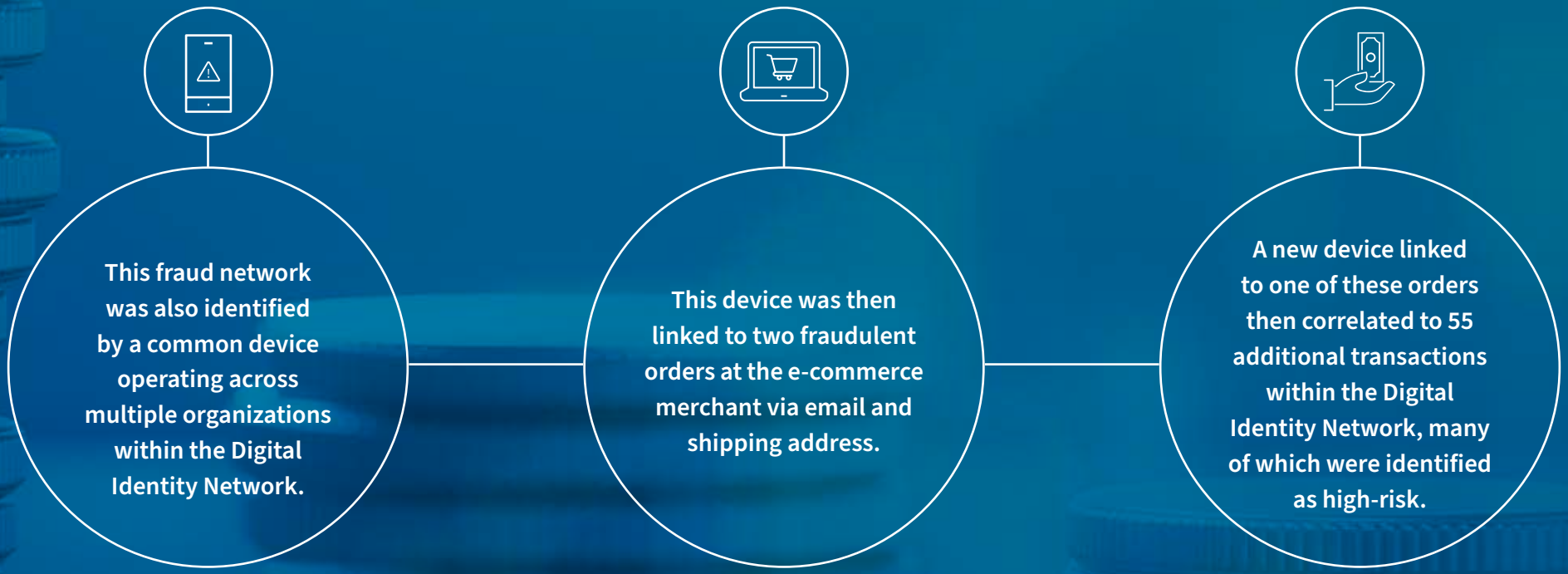
LexisNexis® RISK SOLUTIONS

2. BANK / E-COMMERCE / MARKETPLACE FRAUD NETWORK

Large Networked Fraud Ring Operating Across Multiple Industries, Originating in Retirement Community

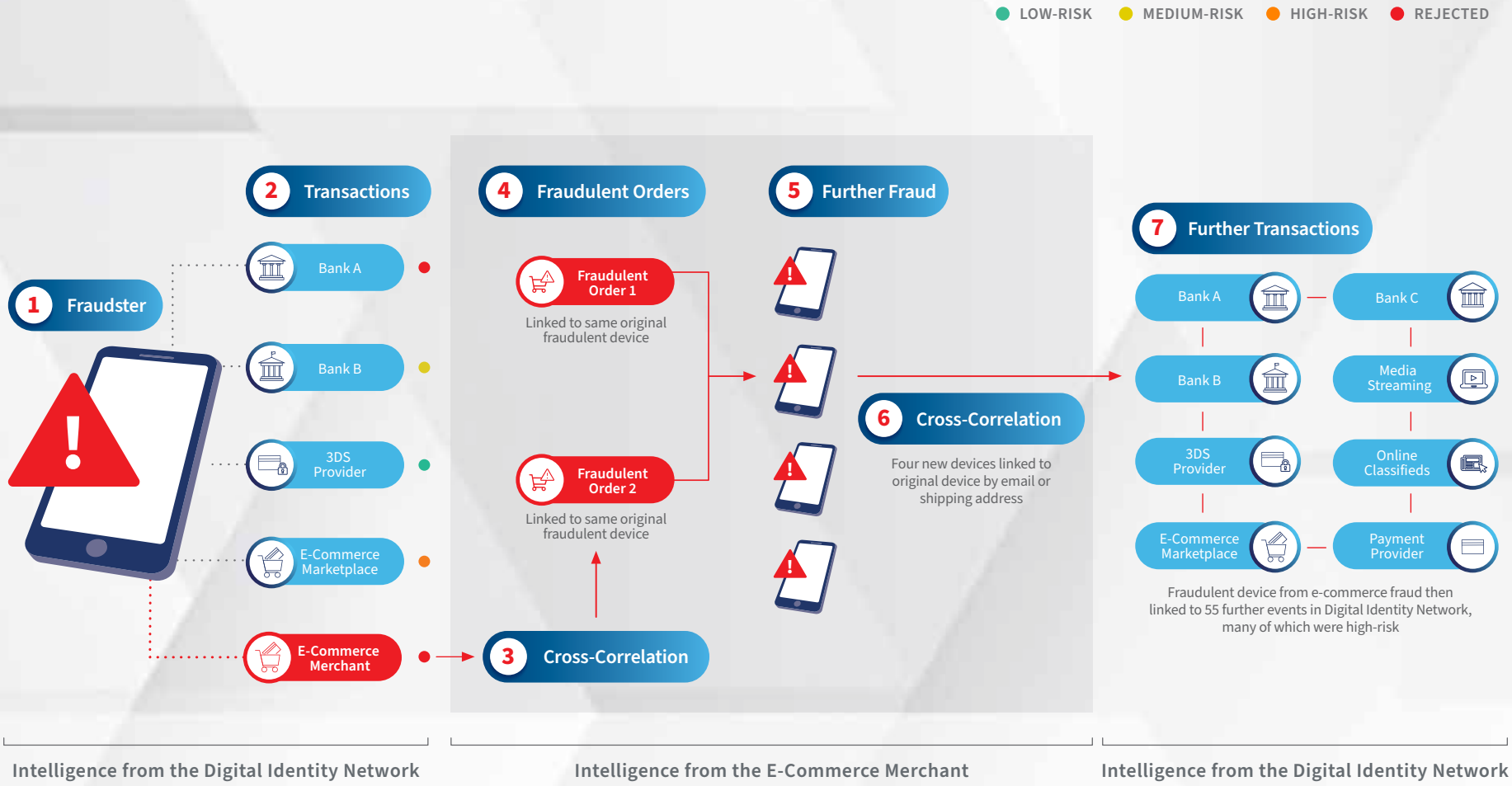
LexisNexis® RISK SOLUTIONS

A REGIONAL VIEW:
ANATOMY OF FRAUD NETWORKS



LexisNexis® RISK SOLUTIONS

COLLABORATION WITH E-COMMERCE MERCHANT REVEALS COMPLEX, NETWORKED FRAUD



LexisNexis® RISK SOLUTIONS

SHARED INTELLIGENCE HELPS DETECT FURTHER NETWORKED, HIGH-RISK BEHAVIOR

1 Fraudster

As with the previous fraud network, another fraudster was tracked carrying out a series of transactions, many of which were high-risk and fraudulent, across multiple organizations within the Digital Identity Network.

2 Transactions

The fraudster attempted a series of logins and online banking payments all on the same day. Many of these were scored as high-risk, and several were rejected.

- *The fraudster then appears to make a card-not-present payment, seen through a 3DS provider in the Digital Identity Network. This is passed as low-risk.*
- *The fraudster then attempts to login twice to an e-commerce marketplace.*
- *Again, each organization assessed the transactions according to their own policies and tolerance for risk.*

3 Cross-Correlation

The e-commerce merchant took the device intelligence from these fraudulent transactions and cross-correlated it to its own network.

4 Fraudulent Orders

This device was associated with two fraudulent orders.

5 Further Fraud

These two fraudulent orders were then associated with a further six fraudulent orders using email addresses and shipping addresses, using four new devices.

6 Cross-Correlation

These devices were then cross-correlated back to the Digital Identity Network.

7 Further Transactions

One of the new devices was found to be associated with 55 further transactions across eight organizations within the Digital Identity Network.

- *Four organizations were those involved in the original fraud network.*
- *A further four organizations were new to the fraud network.*
- *Many of these transactions were marked as high-risk and assumed to be fraudulent.*

LexisNexis® RISK SOLUTIONS

UNDERSTANDING THE MODUS OPERANDI OF COMPLEX FRAUD RINGS

Building Strategies to Mitigate Networked Fraud Risk

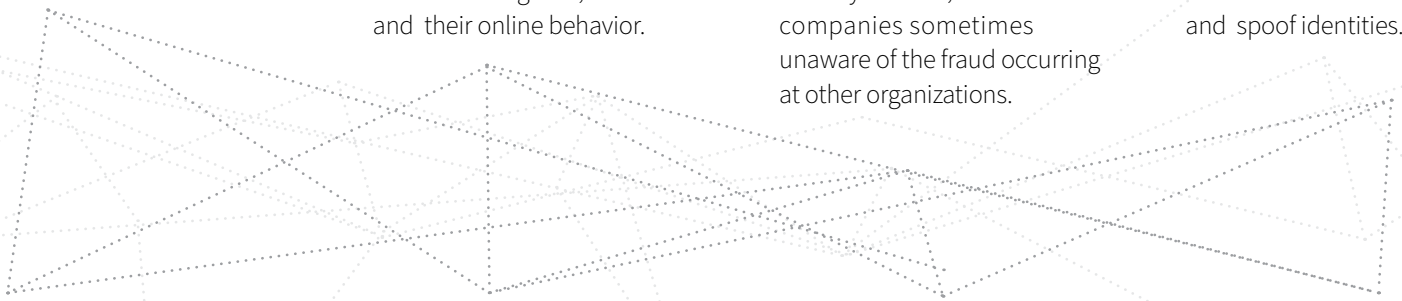
PROBLEMS

CROSS-ORGANIZATIONAL:
Fraudsters work across organizations to maximize their success / monetary exploitation.

COMPLEX DATA:
Fraud networks are complex and expose myriad pieces of digital identity data related to the transacting user, their device and their online behavior.

CROSS-INDUSTRY:
Fraudulent behavior can spider web out from one organization to many, across industries and country borders, with individual companies sometimes unaware of the fraud occurring at other organizations.

SOLUTION VULNERABILITIES:
Fraudsters often use techniques to bypass device fingerprinting, obfuscate their true location and spoof identities.



SOLUTIONS

DATA SHARING:
Businesses need a shared view of risk to better track cross-organizational fraud.

Analyzing data across a shared network enables businesses to track fraudulent and high-risk behavior in near real time.

DIGITAL IDENTITY INTELLIGENCE:
Harnessing digital identity intelligence related to devices, shipping addresses, email addresses and credit cards, provides a holistic view of consumers to better differentiate between trust and risk. Additional transactional data indicators can also help detect anomalous and high-risk behavior before transactions are processed.

FRAUD DETECTION:
The ability to share near real-time intelligence related to confirmed fraud, with trust and context across consortia groups, can provide a near real-time solution to networked fraud. Sharing feedback and intelligence on fraud typologies can also help businesses to adapt their fraud strategies to mitigate evolving fraud trends.

A LAYERED DEFENSE:
Businesses must look to implement layered solutions that are harder for fraudsters to circumvent than individual point solutions. Combining device fingerprinting, behavioral analytics, machine learning and behavioral biometrics, provides a more robust defense to complex fraud.

LexisNexis® RISK SOLUTIONS

04

FRAUD WITHOUT BORDERS

AN INDUSTRY VIEW

Industry Highlights

Industry benchmarking highlights variations in attack patterns by industry.

The media industry sees the most prominent spikes in attack rates.

Media and e-commerce organizations are the most susceptible to identity spoofing.

Financial services organizations are most likely to be targeted by IP spoofing attacks and have seen a growth in account creation attacks.

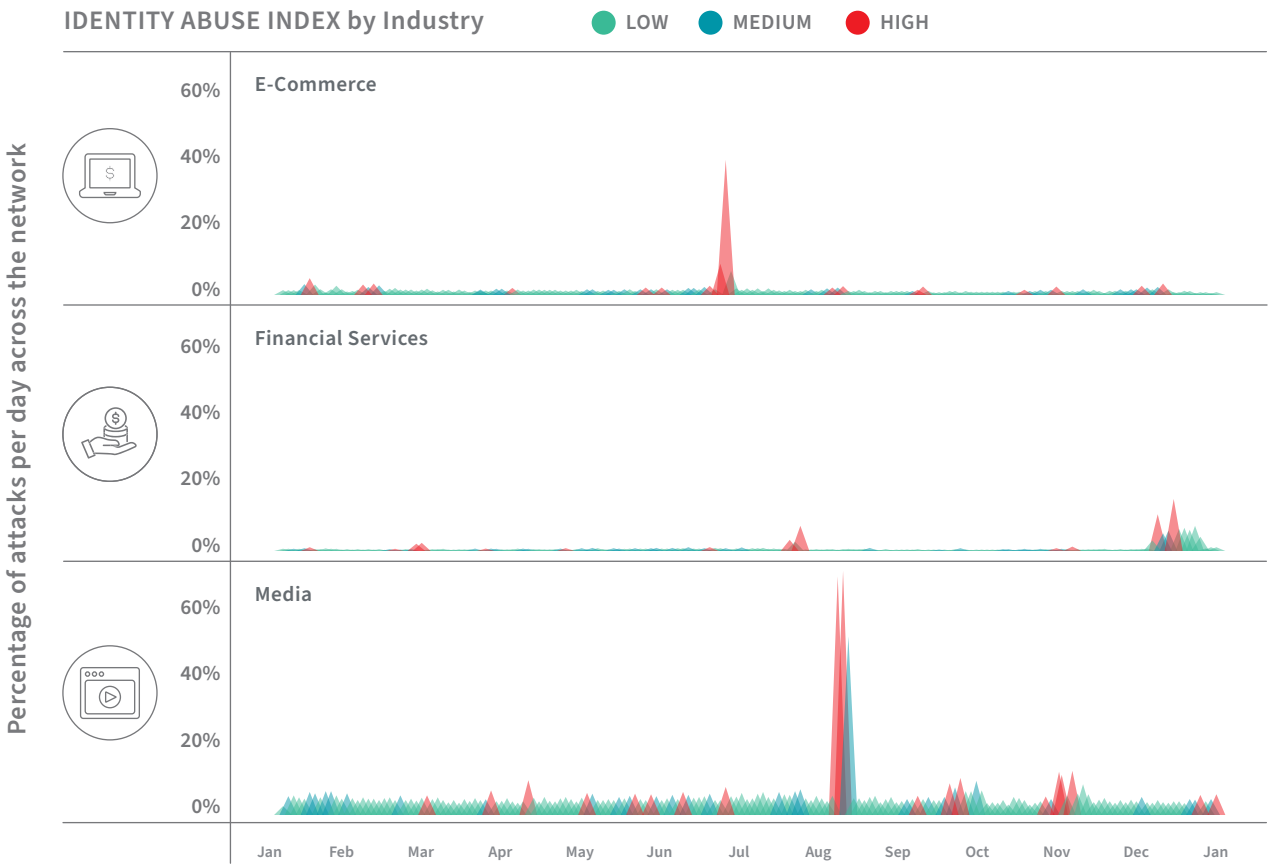
INDUSTRY BENCHMARKING OF FRAUD

Using the Identity Abuse Index to View Variations in Attack Rate by Industry

Despite the fact that both e-commerce and financial services organizations see higher overall attack volumes, the media industry experiences the most prominent peaks in attack rates, as a percentage of total transactions.

Media organizations typically become test beds for stolen identity credentials given that accounts are generally simpler to open and easier to access than accounts in other industries.

The Digital Identity Network sees a high proportion of trusted login transactions for financial services organizations, driven by full service mobile banking apps. As a result, peaks in attacks are less noticeable amongst the high volumes of good transactions, despite the fact that raw attack volumes for financial services are the highest of all three industries.



LexisNexis® RISK SOLUTIONS

VARIATIONS IN ATTACK TYPOLOGIES

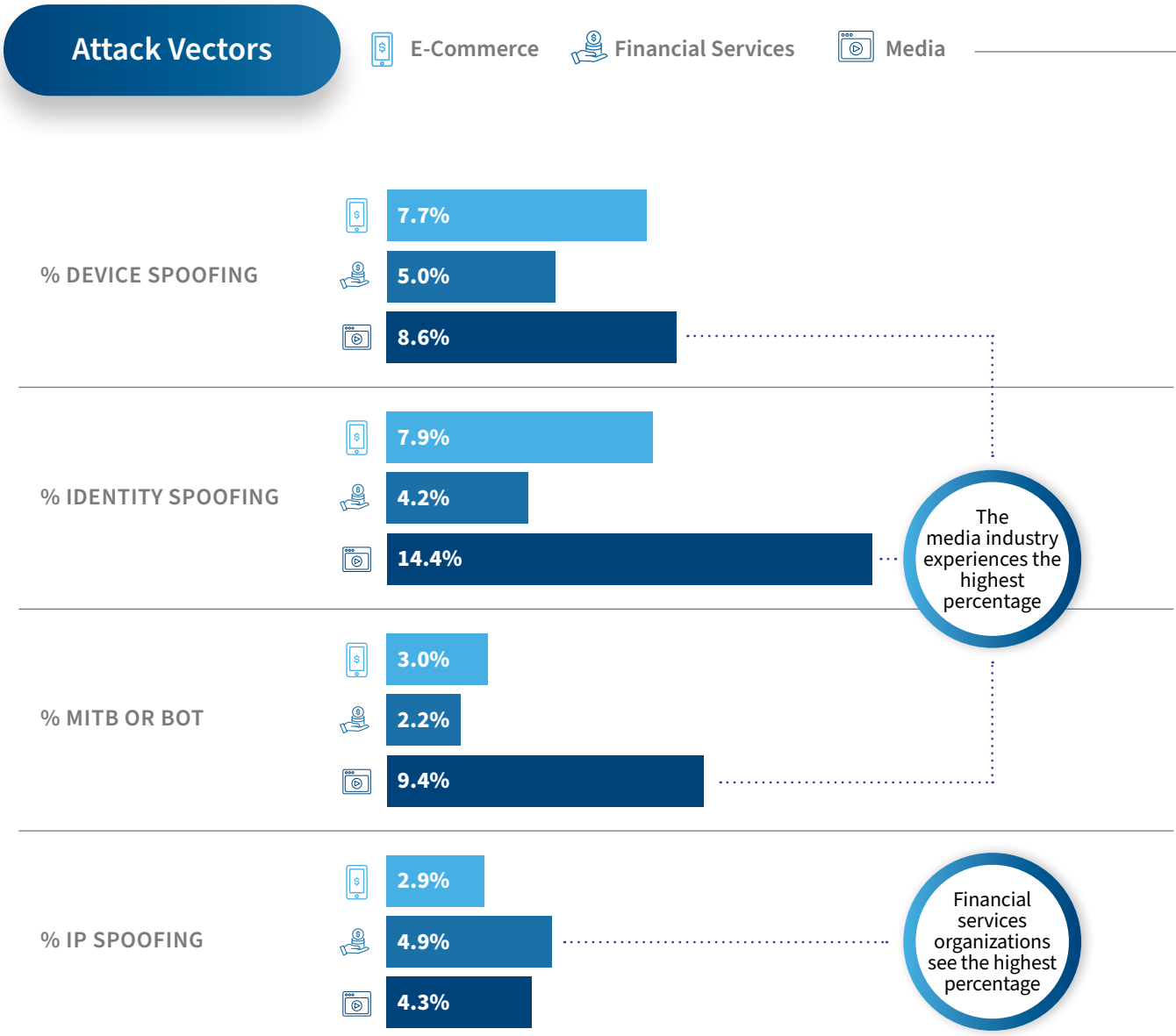
Analyzing Attack Vectors by Industry

Supporting the pattern of attacks visible in the Identity Abuse Index, the media industry experiences the highest percentage of device spoofing, identity spoofing and bot attacks as fraudsters launch automated attacks to mass-test stolen identity credentials.

Financial services organizations see a higher percentage of IP spoofing attacks than any other industry. These attacks may include:

- Fraudsters obfuscating their true location.
- Mule networks attempting to make movement of money across mule accounts harder to track.

Financial services organizations tend to have a strong network of layered fraud defenses, working with law enforcement to detect and block fraud. Fraudsters are therefore working harder to hide their true location to avoid detection and capture.



The bar charts represent percentage of total transactions that were recognized as attacks.

LexisNexis® RISK SOLUTIONS

AN INDUSTRY VIEW:

RISK BREAKDOWN BY INDUSTRY ACROSS THE ONLINE CUSTOMER JOURNEY

Financial Services Organizations Hit by New Account Creation and Payment Attacks

NEW ACCOUNT CREATIONS:

Large Attacks Hit U.S. Financial Services

LOGINS:

The E-Commerce Industry Continues to See Highest Attack Rates

PAYMENTS:

E-Commerce and Financial Services Organizations are Prime Targets for Cashing Out

LexisNexis® RISK SOLUTIONS

Attack Rate by Industry and Use Case

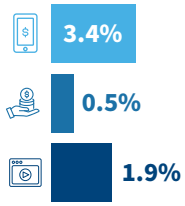
E-Commerce | Financial Services | Media

NEW ACCOUNT CREATIONS

The financial services industry experienced the highest attack rate on new account creation attacks this period, due to sustained bot attacks on U.S. financial services.

This attack rate represents a significant growth in comparison to the first half of 2019.

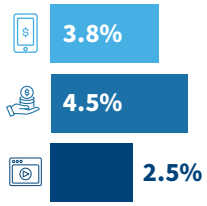
LOGINS



The e-commerce industry continues to be the prime target for fraudsters attempting to take over good user accounts.

These accounts provide an opportunity to access account information, make fraudulent CNP purchases and monetize stolen credit cards.

PAYMENTS



Financial services organizations still offer the best opportunity for fraudsters to monetize fraudulent activity.

However the e-commerce industry has experienced a 46% growth in the payments attack rate year over year, while the attack rate has declined for both financial services and media organizations.

LexisNexis® RISK SOLUTIONS

AN INDUSTRY VIEW:

FRAUD NETWORK ATTEMPTING TO MAXIMIZE SUCCESS ACROSS INDUSTRIES

Network Shows Evidence of Credential Testing Attack

The Digital Identity Network has identified a fraud network that is operating across multiple organizations, spanning all industries.

The fraud network appears to be testing credentials at several loan companies in Latvia, Poland and the UK. Many of these transactions are new account creations and payments, suggesting that the fraud network may be taking out a series of loans and layering these proceeds into other accounts.

Given that a gambling company and retailer appear in this fraud network, it is possible that these organizations are providing the fraud network with an opportunity to cash-out or launder fraudulent funds.

LexisNexis® RISK SOLUTIONS

AN INDUSTRY VIEW:

CROSS-INDUSTRY FRAUD NETWORK

Cross-Over Between E-Commerce, Media and Financial Services Organizations

Anatomy of Fraud Network

900
Devices associated with fraud, cross over with more than one organization.

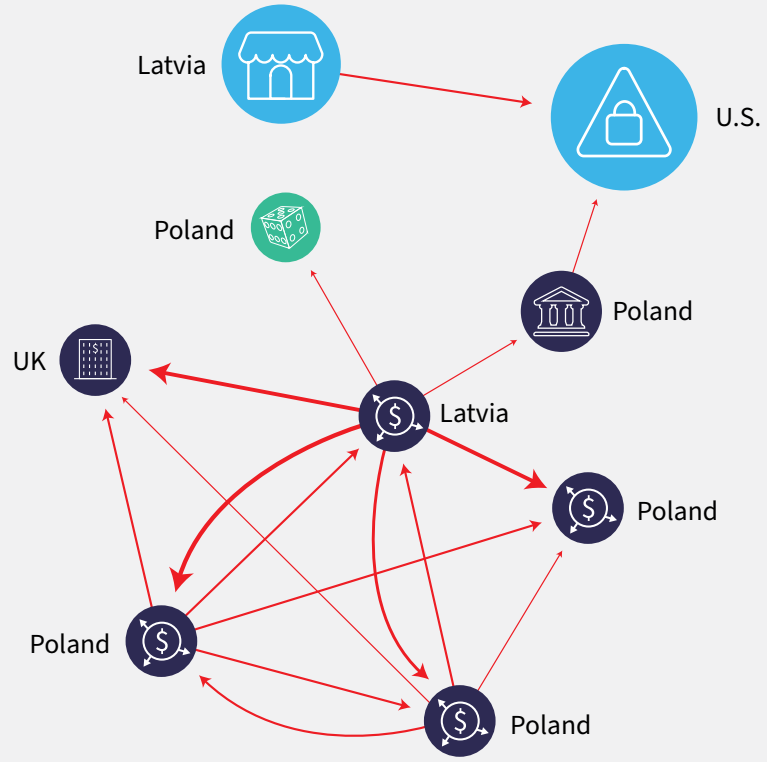
1,400
Cross-organizational events are new account creations.

400
Cross-organizational events are login transactions.

1,000
Cross-organizational events are payment transactions.

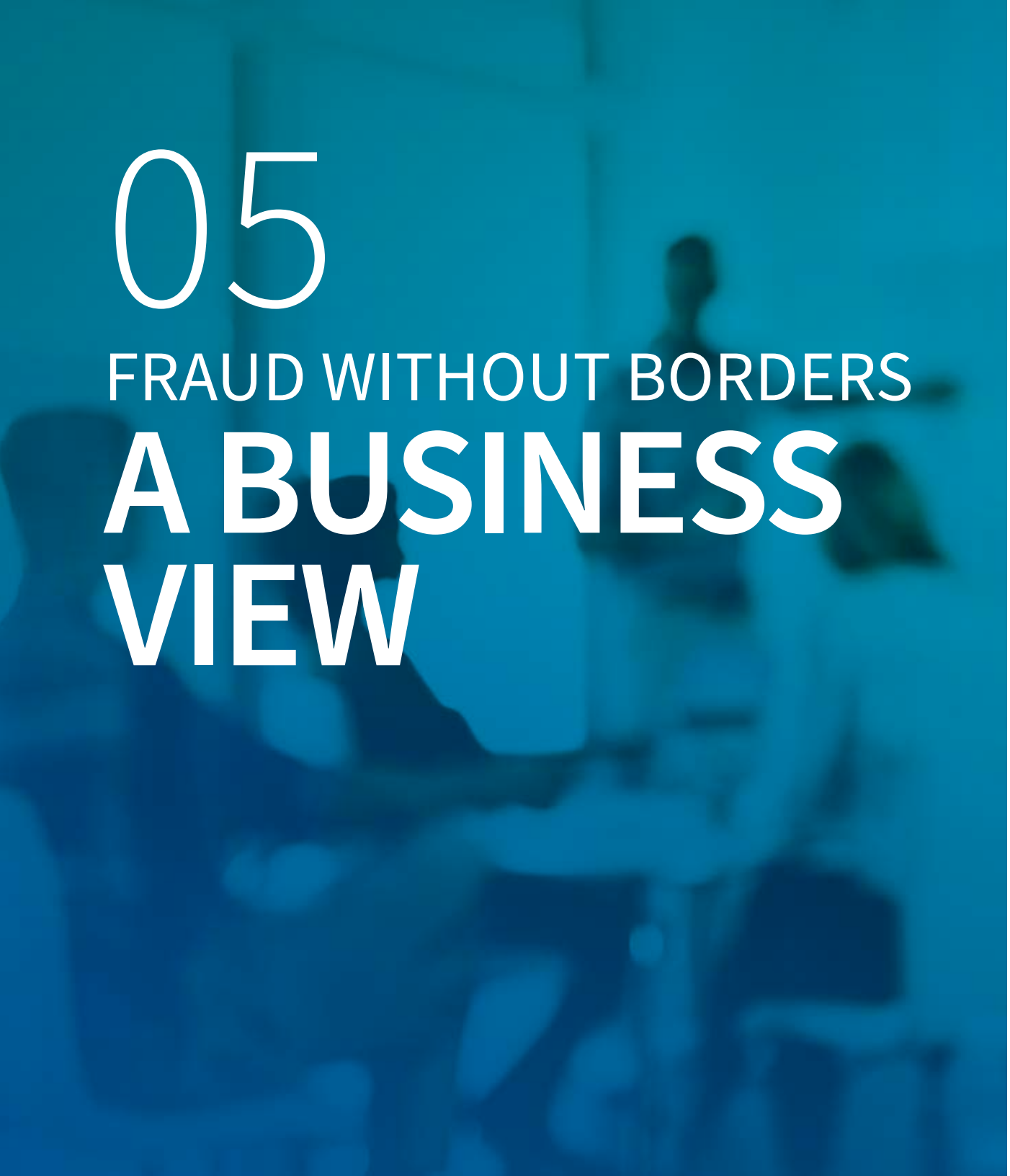
$0.5M
Exposure to fraud at original organization.

$80,000
Exposure to fraud at cross-over organizations in one-month period.



A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud. Less than 10 device overlaps between companies have been removed.

LexisNexis® RISK SOLUTIONS



05

FRAUD WITHOUT BORDERS

A BUSINESS VIEW

Business Highlights

Fraud Stories from Global Digital Businesses

Tracking payments fraud within the UK banking ecosystem.

Synthetic identity fraud ring from the U.S.

Fraudsters operating across e-commerce merchant and travel company.

Detecting bots targeting online marketplace.

ANALYSIS OF PAYMENT FRAUD IN THE UK BANKING ECOSYSTEM

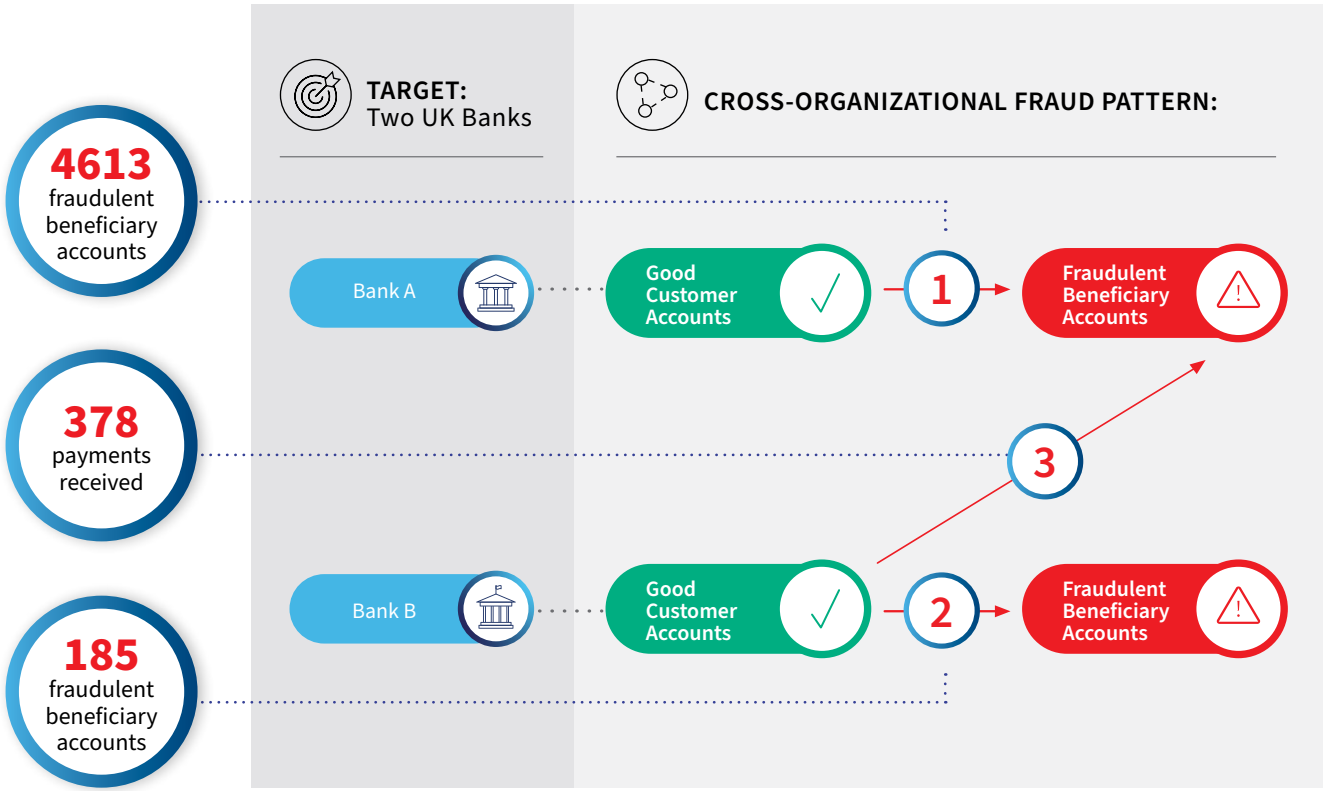
Tracking Payments Between Payer and Beneficiary

This fraud network is maximizing its opportunity for monetary gain by working across multiple UK banks simultaneously:

1. Bank A: **4613** fraudulent beneficiary accounts associated with a fraudulent payment.
2. Bank B: **185** fraudulent beneficiary accounts associated with a fraudulent payment.
3. **378** of Bank A's fraudulent beneficiary accounts received payments from Bank B customers.

Sharing confirmed fraud data in near real time could prevent the fraudulent payments between these two banks.

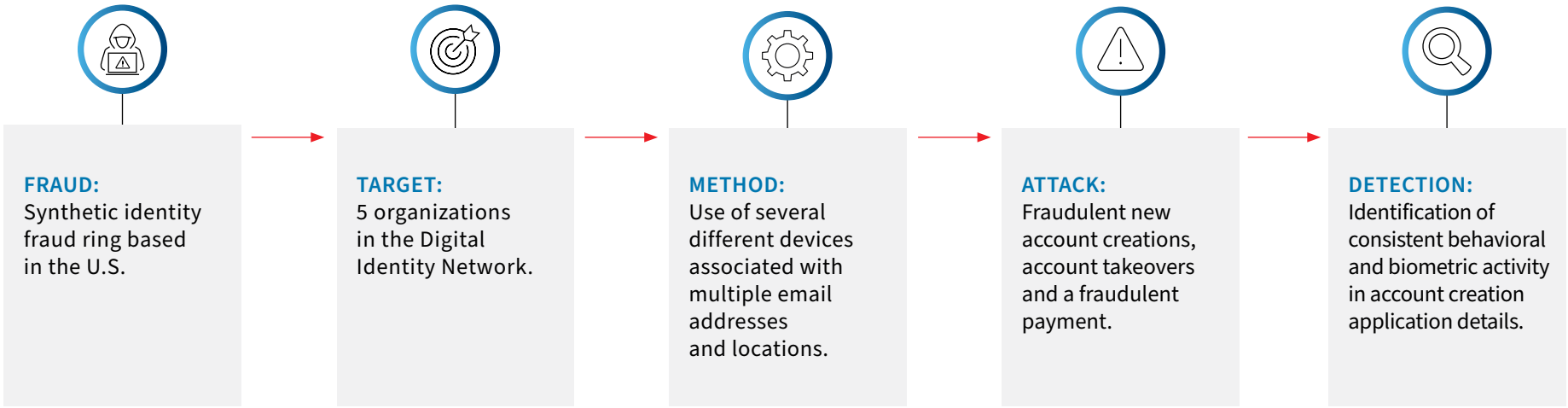
Transaction monitoring capabilities, and the ability to track payments across the payer and recipient (two-party payment modeling), can also share the context of these transactions in a network view. This helps to extend the visibility of linkages to other financial events.



LexisNexis® RISK SOLUTIONS

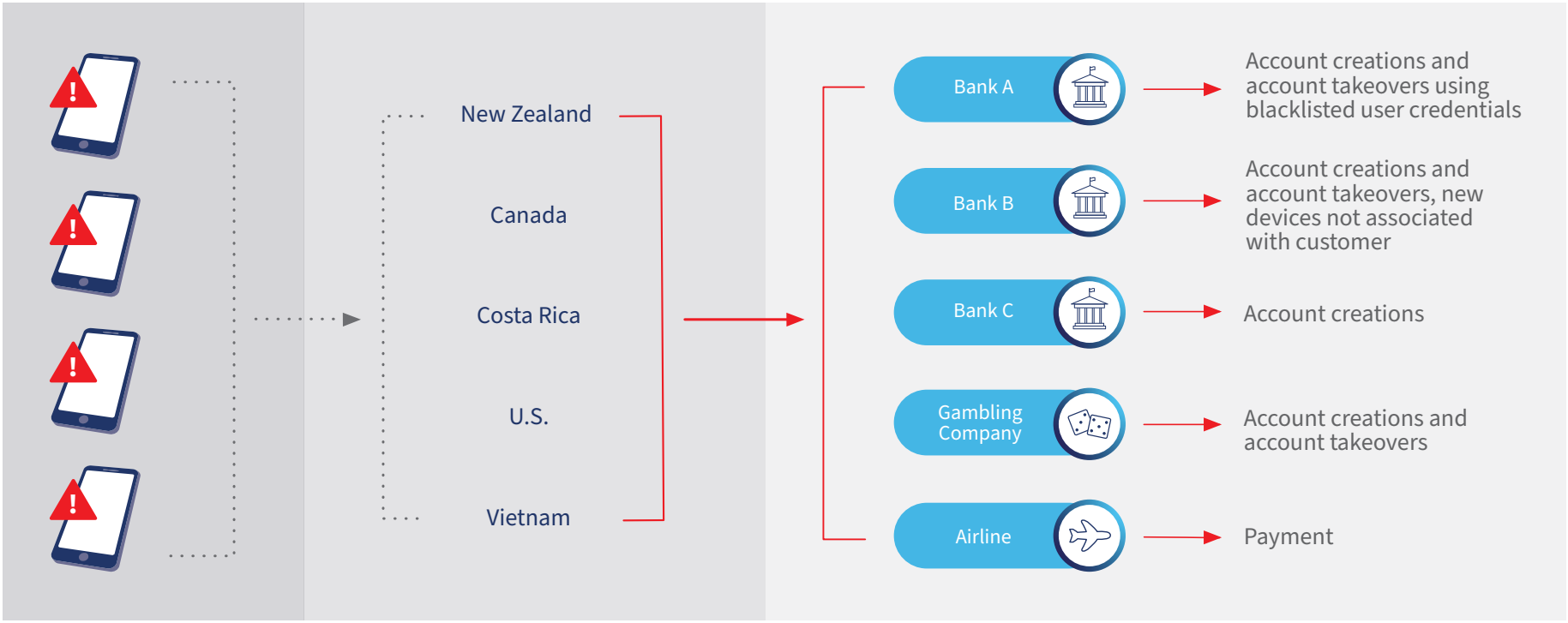
SYNTHETIC IDENTITY FRAUD RING LINKED TO FOUR DEVICES

High-Risk Activity Tracked Across 3 Regions and 5 Different Organizations



LexisNexis® RISK SOLUTIONS

TRACKING FRAUDULENT ACTIVITY ACROSS THE NETWORK



1 Linked Devices

4 Devices linked to 1 IP address and 52 different email addresses

2 Multiple Locations

Devices appear to come from 5 different locations across 3 regions

3 Events in Digital Identity Network

81 events seen at 5 different organizations in the Digital Identity Network

LexisNexis® RISK SOLUTIONS

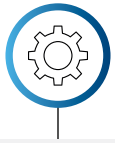
FRAUD TARGETING ECOMMERCE LOYALTY PROGRAM AND TRAVEL COMPANY

Fraudsters Cashing in on Loyalty Accounts and Unclaimed Rewards

TARGET:
Travel Vouchers via E-commerce Customer Loyalty Program

This loyalty program gives customers a variety of rewards to redeem in exchange for loyalty points.

One of the rewards available is vouchers with a local travel company.



METHOD:
Cybercriminals Using Two Key Methods of Attack

Takeover of e-commerce loyalty accounts in order to fraudulently request travel vouchers.

Unauthorized registration of a rewards account in the name of a customer with unclaimed loyalty points, perhaps by a rogue travel agent.

ATTACK:
Change of Details Requests

In the case of the account takeovers the fraudster would login into the good customer account, change the email and/or password on the account then request the loyalty program vouchers.

The new email domains used were those in possession of the fraudster.

A Proxy IP has also been used in the majority of cases.

LexisNexis® RISK SOLUTIONS

ONLINE MARKETPLACE TARGETED BY AUTOMATED BOTS

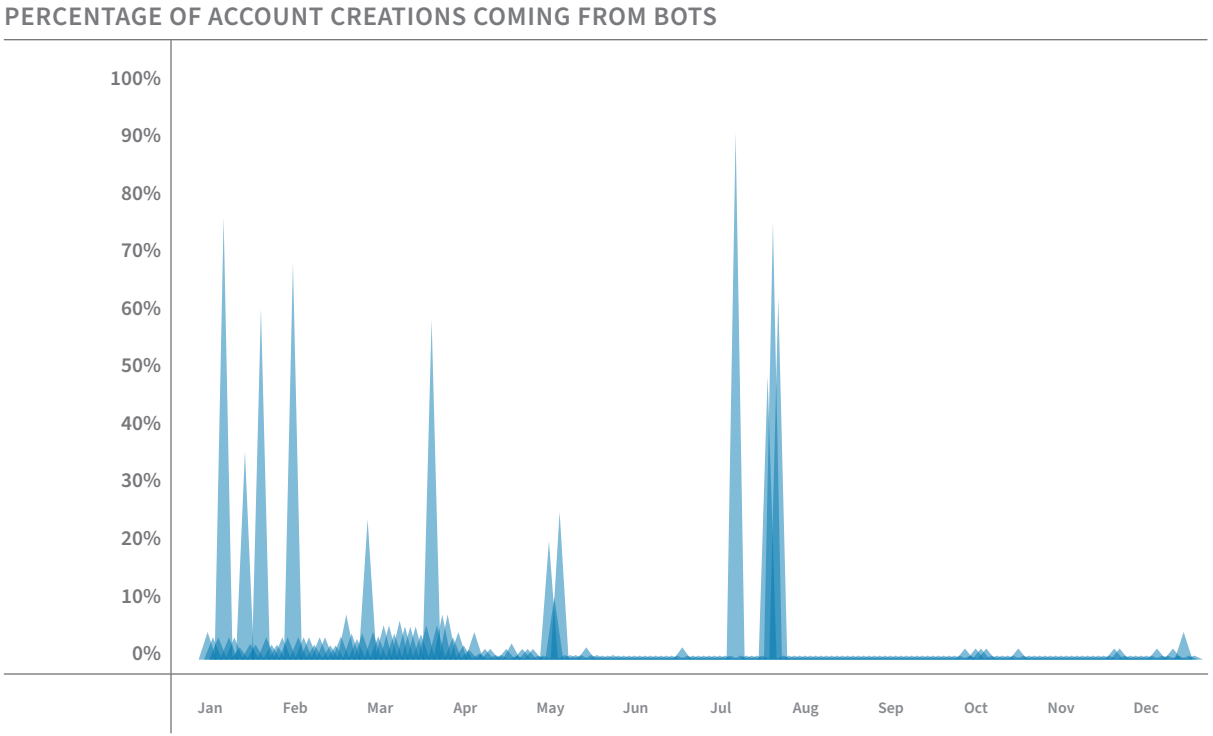
Fraudsters From Russia and Ukraine Attempt to Open Accounts en Masse

FRAUDSTER:
Controlling a large bot from Russia and Ukraine

TARGET:
EMEA-based online marketplace

METHOD:
High velocity account creation attempts using 8,500 different devices and German / Swiss email addresses

ATTACK:
On peak days, over 90% of transaction volume came from bots. During the peak month of July, 30,000 account creation attempts were made from a desktop computer



LexisNexis® RISK SOLUTIONS

06

FRAUD WITHOUT BORDERS

CONSUMER IMPACT

UNDERSTANDING THE IMPACT OF FRAUD ON CONSUMERS

Victims of Fraud Often Stop Using Services and Defect to Competitors

- End users who are victims of fraud are more likely to stop using a service following the fraudulent event, often defecting to a competitor service.
    - Not only does fraud have an immediate monetary impact on the organization, (via chargebacks or reimbursements to innocent consumer), they often then feel the effects of the fraud for months and years to come.
    - For example, large data breaches can irrevocably damage an organization's reputation and therefore consumer base. At the same time a fraudulent event can severely affect the likelihood of a customer to recommend a service to a friend or family member.
- The economic, social and emotional impact on the consumer themselves also has far-reaching effects.
    - Consumers do not always recoup money they lose as a result of fraud, particularly if they were an unwitting participant in a social engineering scam where they authorized a payment.
    - Consumer credit ratings can be severely affected by an identity theft incident, taking time and resources to resolve.

- The Identity Theft Resource Center Survey reports that 7% of identity theft victims consider suicide.
- The Federal Trade Commission reports that older adults can be disproportionately affected by fraud and tend to lose more money than younger victims.

LexisNexis® RISK SOLUTIONS

07 CONCLUSION

Building Next-Generation Fraud Defenses to Detect Complex, Networked Fraud

ANALYZING THE IMPACT OF GLOBAL FRAUD NETWORKS

Sharing Intelligence is Key to Detecting and Blocking Networked Fraud

Detailed analysis of global fraud networks helps to unpack the size, scale and impact of cybercrime on digital businesses and consumers. Businesses must look to layered defenses that harness global shared intelligence to mitigate the impact of this fraud.

Evidence from the Global Fraud Networks:	Protection from the Digital Identity Network:
Fraudsters are working in hyper-connected, global networks, targeting businesses across country borders and across the full spectrum of industries.	Harnessing intelligence from global digital businesses, across industries and transaction types, creates a network of digital identity intelligence that can be used to reliably differentiate between good customers and potential threats in near real time.
Linked organizations can benefit from sharing intelligence about confirmed fraud, because they are being targeted by the same fraudulent digital identity.	The Digital Identity Network gives businesses a shared view of fraud and risk. This includes intelligence relating to online behavior, transaction trust and risk, global blacklists, whitelists and watchlists, as well as targeted industry models.
Several organizations that are part of a larger fraud network could benefit from a consortium style data sharing model.	Linked organizations, either within the same industry, or with similar fraud challenges, can share fraud data with trust and confidence via consortium list functionality, sharing additional context on confirmed fraud attempts. These consortia can be extended across industries and regions, to create larger global consortia to tackle global fraud networks.

LexisNexis® RISK SOLUTIONS

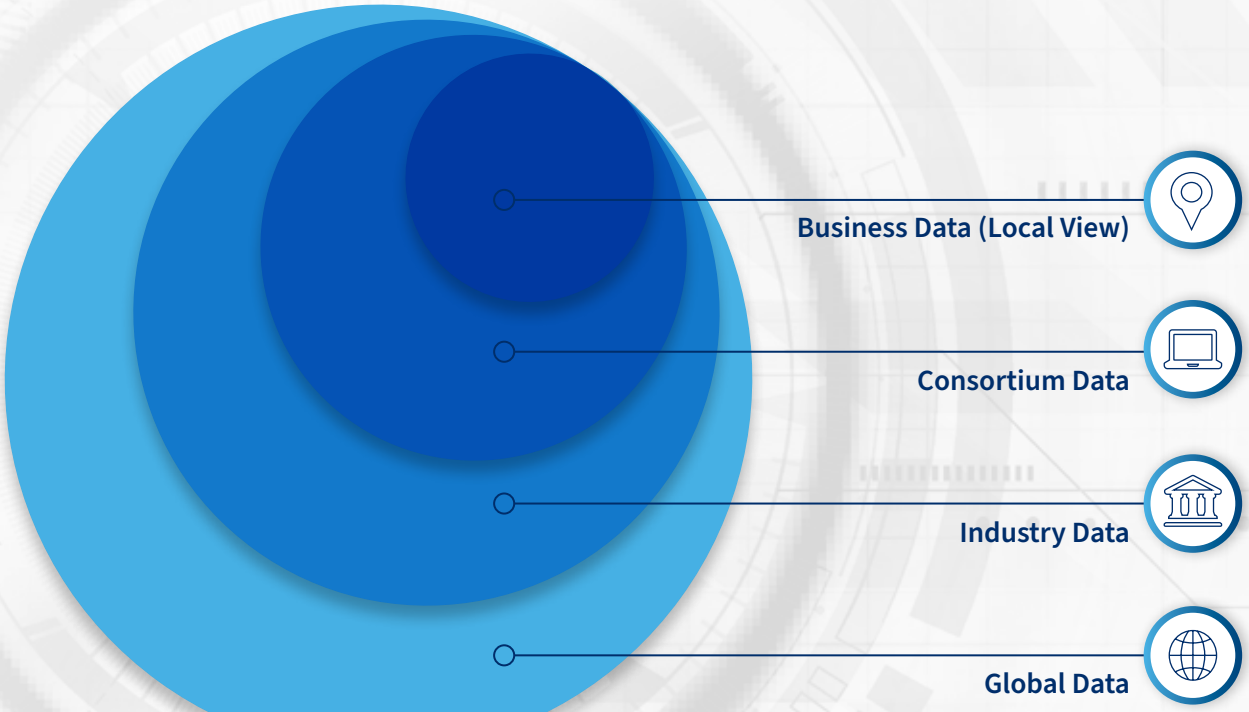
CONCLUSION

USING CONSORTIUM FROM LEXISNEXIS RISK SOLUTIONS TO FIGHT FRAUD

Bringing Organizations Together to Share Intelligence with Trust and Context

Consortium was built as a key enhancement request in order to:

- Facilitate information exchange between LexisNexis Risk Solutions customers.
- Develop focused customer Consortium groups to share information about fraudsters.
- Collectively fight fraud using the Digital Identity Network.
    - Consortium enables businesses with common goals, challenges or fraud risks to share negative and positive data attributes in near real time, across an agreed set of Consortium members and contributors.
    - By providing segmentation through multiple list categories (e.g. account takeover list, mules list) customers can selectively target specific fraud typologies.



SUMMARY

Analysis in this report shows that cybercrime is operating on a global scale in vast, interconnected networks that are unrestricted by regional, country or industry borders.

Given that $40M was at risk from cross-organizational fraud exposure during a one-month period, the likely exposure across the six-month period was $240M.

The individual transactions and attacks that form the building blocks for these networks continue to shift and evolve.

Mobile transaction volumes and attack rates are still experiencing strong growth. Mobile app attack rates have been heavily influenced by global bot activity that can often overwhelm a business's fraud defenses. These bots are vast, automated and come from multiple global geographies and were particularly targeting new account creation transactions during the second half of 2019.

It's clear that cybercrime is a highly networked, complex and ever-evolving beast. Businesses can no longer focus on mitigating individual attacks using point solutions. Fraud solutions should align with the fraud typologies they need to defend against: networked, layered, inter-connected and operating without borders.

The Digital Identity Network helps businesses to make near real-time risk decisions that harness digital identity and biometrics intelligence from thousands of global digital businesses, across millions of daily transactions, and billions of data points. A network without borders to defend against fraud without borders.

Meanwhile the next generation of networked fraud detection capabilities continues to evolve. This includes:

- The development of payment network profiling, linkage and network visualizations.
- Advanced behavioral biometrics capabilities that expose inherent user behaviors without compromising privacy, or introducing unnecessary friction.
- Cross-organizational / cross-industry data sharing via dedicated consortia.
- Network identification of first, second and third-party fraud risks.
- Next-generation bot data management and risk intelligence signals.

It is in the layering of these market-leading innovations that a true network of fraud defenses can be built to tackle the most complex and constantly growing global fraud networks.

LexisNexis® RISK SOLUTIONS

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.

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.

E-commerce includes retail, airlines, travel, marketplaces, ticketing 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 computers received and processed by the LexisNexis® Risk Solutions 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® Risk Solutions 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 Risk Solutions 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 our Digital Identity Intelligence to life; helping 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.

LexisNexis® RISK SOLUTIONS

SUMMARY METHODOLOGY

Overall Report

- The LexisNexis Risk Solutions Cybercrime Report is based on cybercrime attacks detected by the LexisNexis Digital Identity Network (the Digital Identity Network) from July – December 2019, during near real-time analysis of consumer interactions across the online journey, from new account creations, to logins and payments.
- The Digital Identity Network provides unique insight into transaction patterns and emerging cybercrime threats.
- 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.

Network Linking

- Fraud performance data taken from September 2019, based upon devices identified between August 2019-October 2019 and recorded as fraudulent in the Network between August 2019-November 2019.
- Monetary exposure calculated on observed payment transactional value at risk in September 2019, based upon the identification of all transactions associated with that confirmed fraud device during the period. Does not include any financial values at risk from customers who do not provide payment transactional data.

LexisNexis® RISK SOLUTIONS

DATA PROCESSED AND ANALYZED

The overall volume of transactions processed by the Digital Identity Network during the period is significantly higher than the 19.1 billion transactions recorded for the purposes of this report. Analysis only considers customer transactions analyzed for risk by LexisNexis® ThreatMetrix®. All other API calls to the ThreatMetrix platform (e.g. feedback data, test transaction, etc.), are excluded.

From the 19.1 billion transactions analyzed globally from July-December 2019, LexisNexis Risk Solutions uses subsets to conduct detailed analysis.

The customer journey volume analysis excludes transaction and attack volumes listed as "other", e.g. change of details and internal transfers.

The total transaction and attack volumes for the four key regions exclude some transactions that do not have an IP address, and therefore cannot be categorized by region. They also exclude the transactions from some countries that are not part of one of the four key regions.

Differentiating between automated bot attacks and sophisticated human-initiated attacks:

- LexisNexis Risk Solutions differentiates between simple threats, like automated bots and human-initiated/ sophisticated attacks (401 million) based on the profiling data within our Network.
- For the sophisticated attacks, LexisNexis Risk Solutions considers a subset of 15.6 billion of the 19.1 billion transactions. These are categorized as "known sessions" related to individual events.
- This excludes a variety of events; for example, high volume bot traffic (bad and good/tolerated bots, such as auction bots), events that failed to gather any digital intelligence due to unsuccessful profiling, and customers with attack rates considered to be outliers.

LexisNexis® RISK SOLUTIONS

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: +55 11 4862 3831
Mexico: +52 55 4755 0043

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 Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London.

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

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in near real time. LexisNexis, LexID, and the Knowledge Burst logo are registered trademarks of RELX. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc.

Learn more at risk.lexisnexis.com/FraudandIdentity