LexisNexis®
RISK SOLUTIONS

THE NEW CYBERCRIME LANDSCAPE

GLOBAL RISKS, REGIONAL TRENDS, INDUSTRY OPPORTUNITIES

The LexisNexis® Risk Solutions Cybercrime Report
July to December 2020

01 INTRODUCTION

TABLE OF CONTENTS

01 **INTRODUCTION:** **2**

Unprecedented Global Change Creates New Opportunities for Cybercriminals **3**

2020: Full Year Review **5**

THE CYBERCRIME LANDSCAPE: JULY-DECEMBER 2020 ANALYSIS

02 Global Risks **6**

03 Across the Customer Journey **21**

04 Regional Trends **26**

05 Industry Opportunities **37**

06 **CYBERCRIME IN A PANDEMIC:** **45**

Consumer Trends and Fraud Typologies **46**

Fraud Risk by Age **48**

07 **CONCLUSION:** **50**

Predictions for the Year Ahead: The Opportunity for Digital Businesses **51**

08 **GLOSSARY, METHODOLOGY, CONTACT DETAILS** **52**

UNPRECEDENTED GLOBAL CHANGE CREATES NEW OPPORTUNITIES FOR CYBERCRIMINALS

During a year of irrevocable change, cybercriminals have remained consistent. Looking for new opportunities, isolating targets that will deliver the most lucrative gains, and heaping additional pressure on global businesses that were forced to adapt and evolve in the face of unprecedented demand.

Several new lines of credit were heavily targeted. Fraudsters also preyed on consumer anxiety, with pandemic-related scams that offered products and services that were either in demand, or in short supply. Pymnts.com, for example, reported that fraud rates increased 55% since the beginning of the pandemic*, while Experian claimed that UK Fraud rates rose 33% during the first COVID-19 lockdown in April**.

This growth in fraud has not been recorded across all digital businesses however; many established platforms have actually reported a fall in attack levels during 2020. Organizations that are part of the LexisNexis® Digital Identity Network® have, for example, seen a significant reduction in attack rates year-over-year. Well established, layered fraud defenses seem to be a significant deterrent for cybercriminals, who instead appear to have turned their attention to new opportunities that have been created by the global pandemic.

Despite reduced attack rates recorded across businesses in the Digital Identity Network®, pernicious attack vectors persist:

- Automated bot attacks continue to be widespread, recorded across global regions and attacking a wide variety of industries and use cases to mass test identity credentials. They offer fraudsters a cheap, quick and effective method of initial attack.
- Likewise, new account creations continue to see high attack rates, representing a key point of entry for fraudsters looking to monetize credentials harvested from data breaches.

The pandemic has brought many additional users online. New analysis in this report shows that the youngest age group of under 25-year-olds are most vulnerable to fraud attacks, while the oldest age group stands to lose the most money. This stark risk at either end of the spectrum puts the need to protect both new-to-digital and vulnerable customers high on the priority list of every global digital business.

* https://www.pymnts.com/fraud-prevention/2021/swap-data-analytics-holiday-fraud/

** https://www.experianplc.com/media/news/2020/fraud-rate-rises-33-during-covid-19-lockdown/

UNPRECEDENTED GLOBAL CHANGE CREATES NEW OPPORTUNITIES FOR CYBERCRIMINALS

Regardless of the many uncertainties businesses face in 2021, they can be sure that their end users will continue to demand access to goods and services wherever and whenever they choose:

- eCommerce merchants, for example, must look to prioritize holistic, omni-channel customer experiences. Routes to purchase are increasingly converging as in-store experiences are being either replaced by, or combined with, digital offerings. Customer recognition across this entire journey becomes more critical than ever.
- Likewise, the diversification of digital payment solutions that are evolving to meet growing consumer demand, places the onus on reliable authentication methods that can detect the use of stolen and spoofed credentials.

In this landscape of rapid change, digital identity intelligence emerges as one of the most precious assets for both consumers and businesses. Online digital identities can adapt and evolve as each individual consumer transacts online, building a digital footprint of their behavior, transaction history and device intelligence.

When this intelligence is crowdsourced across global digital businesses, and updated in near real time, it offers an unparalleled view of trust and risk. For consumers, this means a low-friction online experience as businesses are better able to recognize trusted, returning customers. At the same time, organizations can identify behavior that deviates from this trusted profile. When layered with physical identity and authentication solutions, as well as behavioral biometrics data, this approach can provide a robust, and future-proofed, fraud strategy.

2020: FULL YEAR REVIEW

A Summary of Transactions and Attacks January-December 2020

The forced consumer shift to digital channels drove rapid growth in trusted transactions, with an overall decline in attacks on businesses in the Digital Identity Network. Growth economies contributed the largest growth in attack volumes. The analysis below represents the full year summary of transaction and attack patterns.

TRANSACTIONS PROCESSED

47.1B — **35.5B** in 2019

Mobile transaction penetration:

67% — **65%** in 2019

IDENTITY SPOOFING
Most prevalent attack vector

HUMAN-INITIATED ATTACKS

495M — **679M** in 2019

Percentage of attacks coming from a mobile device:

56% — **55%** in 2019

Largest attacker by volume:

United States

Largest growth in attacks from:

1. Guatemala
2. Bahrain
3. Zimbabwe

AUTOMATED BOT ATTACKS

2.1B — **2.0B** in 2019

Largest attacker by volume:

United States

Largest growth in attacks from:

1. Isle of Man
2. United Arab Emirates
3. Nigeria

02

THE CYBERCRIME LANDSCAPE:

JULY-DECEMBER 2020

GLOBAL RISKS

GLOBAL HIGHLIGHTS: JULY-DECEMBER 2020

TRANSACTIONS

+29% ▲
growth in global transaction volume year-over-year (YOY):

▲ **+29%**
growth in financial services transactions.

▲ **+38%**
growth in eCommerce transactions.

▲ **+9%**
growth in media transactions.

HUMAN-INITIATED ATTACKS

-58% ▼
decline in human-initiated attack rate YOY:

▼ **-58%**
decline in financial services attack rate.

▼ **-58%**
decline in eCommerce attack rate.

▼ **-54%**
decline in media attack rate.

AUTOMATED BOT ATTACKS

-2% ▼
decline in automated bot attacks YOY:

▼ **-8%**
decline in financial services bot volume.

▲ **+32%**
growth in eCommerce bot volume.

▲ **+10%**
growth in media bot volume.

GLOBAL TRANSACTION PATTERNS IN NUMBERS

COVID-19 Has Created New Opportunities for Digital Businesses and Pushed More Consumers Online

In the last 6 months of 2020, transaction volume maintained strong growth in the Digital Identity Network, as businesses and consumers continued to move online.

Although the volume of new account creations declined YOY, this was mainly driven by an extremely high volume of new account creation attacks targeting financial services at the end of 2019.

Mobile continues to facilitate broad access to goods and services, with nearly 7 in every 10 transactions coming from a mobile device.

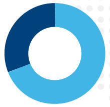
Businesses will progressively need to prioritize not just a digital-first- but a mobile-first-strategy, to service consumers who either rarely use, or don't have access to, a desktop device.

TRANSACTIONS PROCESSED JULY-DECEMBER 2020

24.6B .... Growth YOY **+29%** ▲

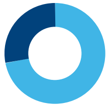
TRANSACTIONS SPLIT BY CHANNEL

Desktop / **Mobile**



31% **69%** .... Growth YOY **+2%** ▲

Mobile Browser / **Mobile App**



28% **72%**

TRANSACTIONS SPLIT BY USE CASE*

		Growth/ Decline YOY
New Account Creations	495M	-43% ▼
Logins	17B	+26% ▲
Payments	4.3B	+34% ▲

Remaining transaction volume made up of non-core use cases such as password reset and details change transactions.

GLOBAL ATTACK PATTERNS IN NUMBERS

Attack Volumes Continue to Decline in the Digital Identity Network®

HUMAN-INITIATED ATTACKS

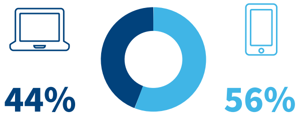
Despite myriad fraud risks reported in the media, organizations in the Digital Identity Network have seen a decline in attacks July-December 2020.

Mobile browser transactions continue to see the highest rate of attack, while mobile app transactions are attacked at the lowest rate.

ATTACK VOLUME

235M — Decline YOY **-42%** ▼

Attack Split by **Desktop** / Mobile



Percentage of attacks coming from mobile devices has decreased YOY

-16% ▼

ATTACK RATE

		Decline YOY
⚠ Overall	1.1%	-58% ▼
Desktop	1.6%	-41% ▼
Mobile Browser	2.3%	-45% ▼
Mobile App	0.4%	-79% ▼

AUTOMATED BOT ATTACKS

Both the eCommerce and media industries experienced a growth in automated bot volume July-December 2020.

While financial services organizations saw an overall decline in bot volume, the absolute volume of attacks targeting this industry remains extremely high.

ATTACK VOLUME

1.2B — Decline YOY **-2%** ▼

		Growth/ Decline YOY
Financial Services	812M	-8% ▼
eCommerce	207M	+32% ▲
Media	170M	+10% ▲

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.

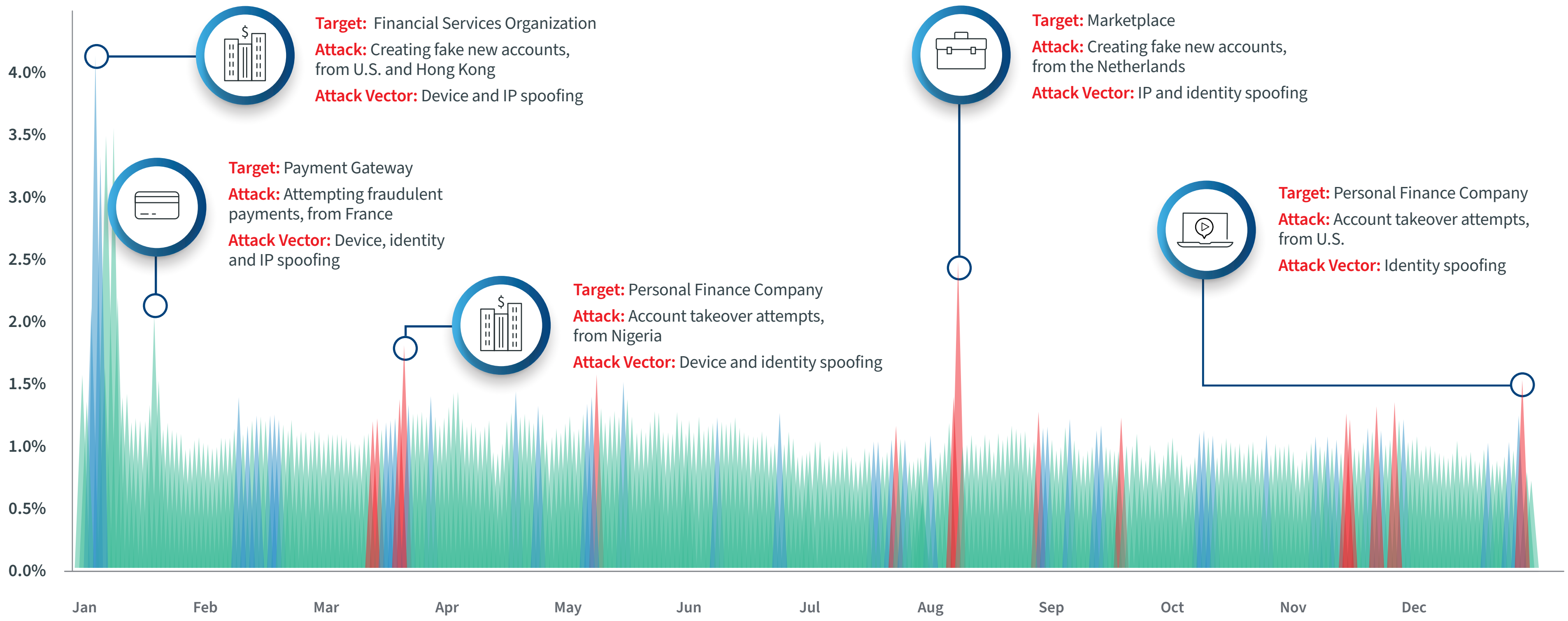
IDENTITY ABUSE INDEX

Bots Remain Method of Choice for Identity Testing Across the Full Spectrum of Use Cases

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

IDENTITY ABUSE INDEX

🟢 LOW 🔵 MEDIUM 🔴 HIGH



Target: Financial Services Organization
Attack: Creating fake new accounts, from U.S. and Hong Kong
Attack Vector: Device and IP spoofing

Target: Payment Gateway
Attack: Attempting fraudulent payments, from France
Attack Vector: Device, identity and IP spoofing

Target: Personal Finance Company
Attack: Account takeover attempts, from Nigeria
Attack Vector: Device and identity spoofing

Target: Marketplace
Attack: Creating fake new accounts, from the Netherlands
Attack Vector: IP and identity spoofing

Target: Personal Finance Company
Attack: Account takeover attempts, from U.S.
Attack Vector: Identity spoofing

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

LARGEST CONTRIBUTORS TO HUMAN-INITIATED ATTACKS, BY VOLUME

Saudi Arabia Joins List of Top 10 Global Attackers by Country of Origin

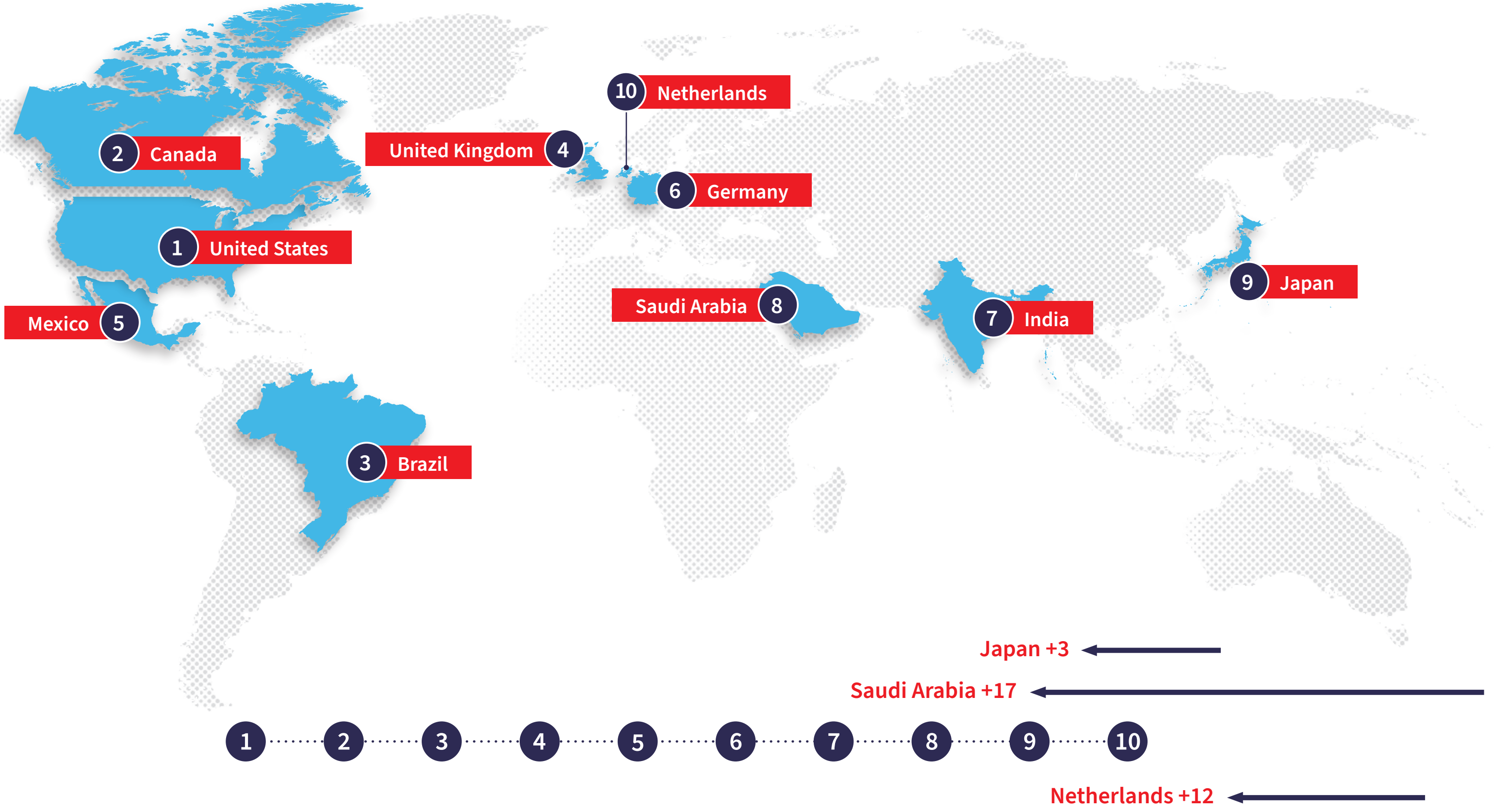
Human-Initiated Attacks

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

Brazil and Mexico both remain on the top 5 list of global attackers by country of origin – Mexico appeared on the list for the first time in 2019 – further establishing LATAM as a region generating a high volume of cyberattacks.

In comparison to the same period last year:

- Saudi Arabia has moved 17 places up the list.
- Netherlands has moved 12 places up the list.
- Japan has moved 3 places up the list.



LARGEST ORIGINATORS OF AUTOMATED BOT ATTACKS, BY VOLUME

Ireland, Australia and Netherlands All Record Significant Growth in Bot Attack Originations, Year-Over-Year

Automated Bot Attacks

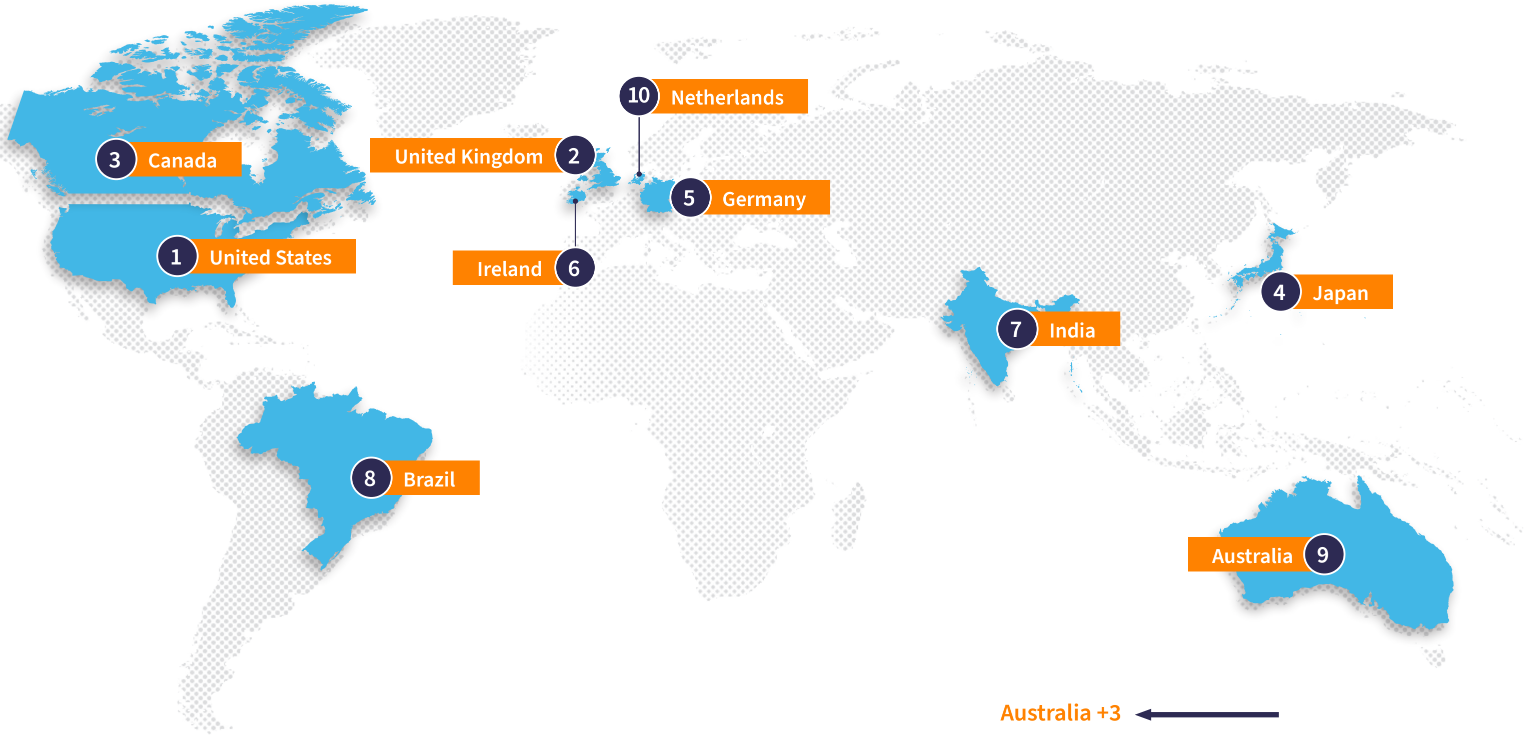
Brazil rejoins the list of top 10 bot attack originators after slipping down the list in the first half of 2020.

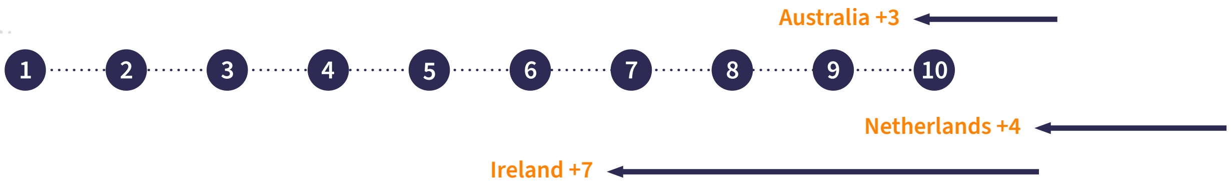
The re-emergence of Brazil as a large originator of bot attacks means that all 4 global regions are once again represented on the top 10 list.

APAC, LATAM and North America have all recorded a growth in bot volume July-December 2020 in comparison to the first half of the year.

In comparison to the same period last year:

- Ireland has moved 7 places up the list.
- Netherlands has moved 4 places up the list.
- Australia has moved 3 places up the list.





FRAUDSTERS LEVERAGE THE POWER OF NETWORKS TO FACILITATE ATTACKS

Hyperconnected Networks Continue to Target Multiple Industries and Organizations

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

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

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

The analysis in this report includes:

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

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

LARGE NORTH AMERICAN FINANCIAL SERVICES NETWORK BEARS HALLMARKS OF MULE ACTIVITY

The visualization on the following page shows a live fraud network targeting the financial services industry, operating across several U.S. and Canadian financial services organizations.

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; however, there is a strong pattern of fraud tied to devices, indicating the same fraudster or fraud ring operating across multiple banks, digital wallets, and lending organizations.

This pattern of fraud is characteristic of mule behavior as mule herders move money across multiple accounts to avoid detection.

NETWORK IN NUMBERS

100,000+

Events linked to confirmed fraud recorded at a source organization.

At least $1.5M

Fraud blocked.

500,000+

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

At least $8.7M

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

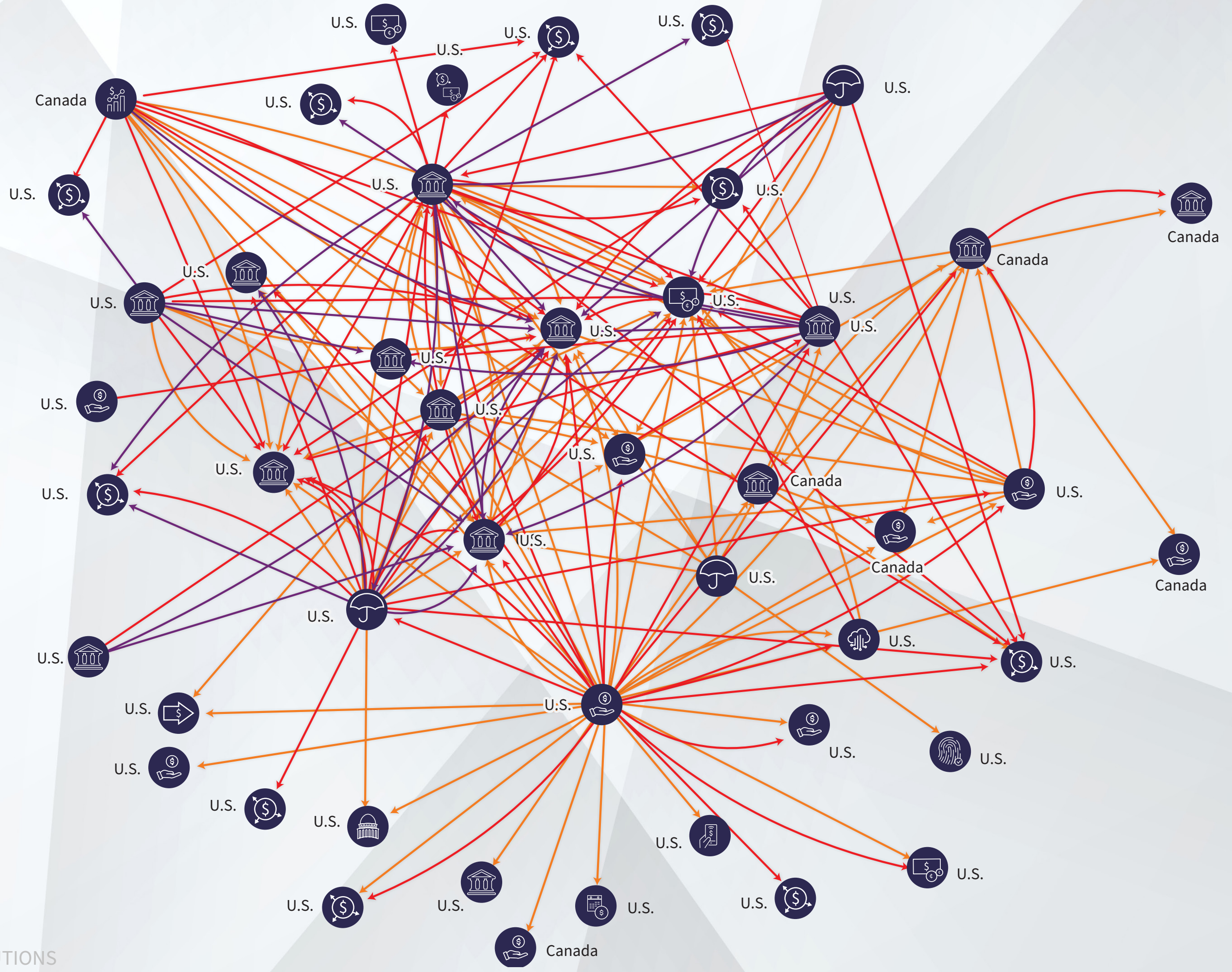
See next page for fraud network visualization

North America includes the U.S. and Canada. Mexico is part of the LATAM region.

NORTH AMERICAN FRAUD NETWORK SHOWS STRONG PATTERN OF DEVICE-BASED CROSS-ORGANIZATIONAL FRAUD

ENTITIES:

- 🟧 DEVICE
- 🟥 EMAIL
- 🟪 TELEPHONE



FINANCIAL SERVICES:

- PAYMENT GATEWAY
- PERSONAL FINANCE
- GOVERNMENT
- LENDING
- STOCK BROKER
- INSURANCE
- DIGITAL WALLET
- BANK
- IDENTITY VERIFICATION
- REMITTANCE
- PAYROLL

Less than 100 entity overlaps between companies have been removed.

North America includes the U.S. and Canada. Mexico is part of the LATAM region.

PAYMENTS FRAUD NETWORK RECORDED ACROSS MULTIPLE ECOMMERCE RETAILERS IN EMEA

The visualization on the following page shows a live fraud network targeting the eCommerce industry, operating across:

- Retailers, a marketplace and payment gateway in Germany
- A retailer and travel organization in France
- A retailer in the Netherlands
- A marketplace in Spain
- A loyalty program in United Arab Emirates
- A retailer in Latvia
- A retailer in Italy

As with the previous network, each arrow illustrates an entity associated with a confirmed fraud event at one organization crossing over to another organization in the Digital Identity Network. However, this fraud network sees a higher proliferation of fraudulent events connected through email addresses.

This shows groups of fraudsters working together to target multiple retailers, using shared stolen credentials.

NETWORK IN NUMBERS

2,000+

Events linked to confirmed fraud recorded at a source organization.

At least $750K

Fraud blocked.

3,000+

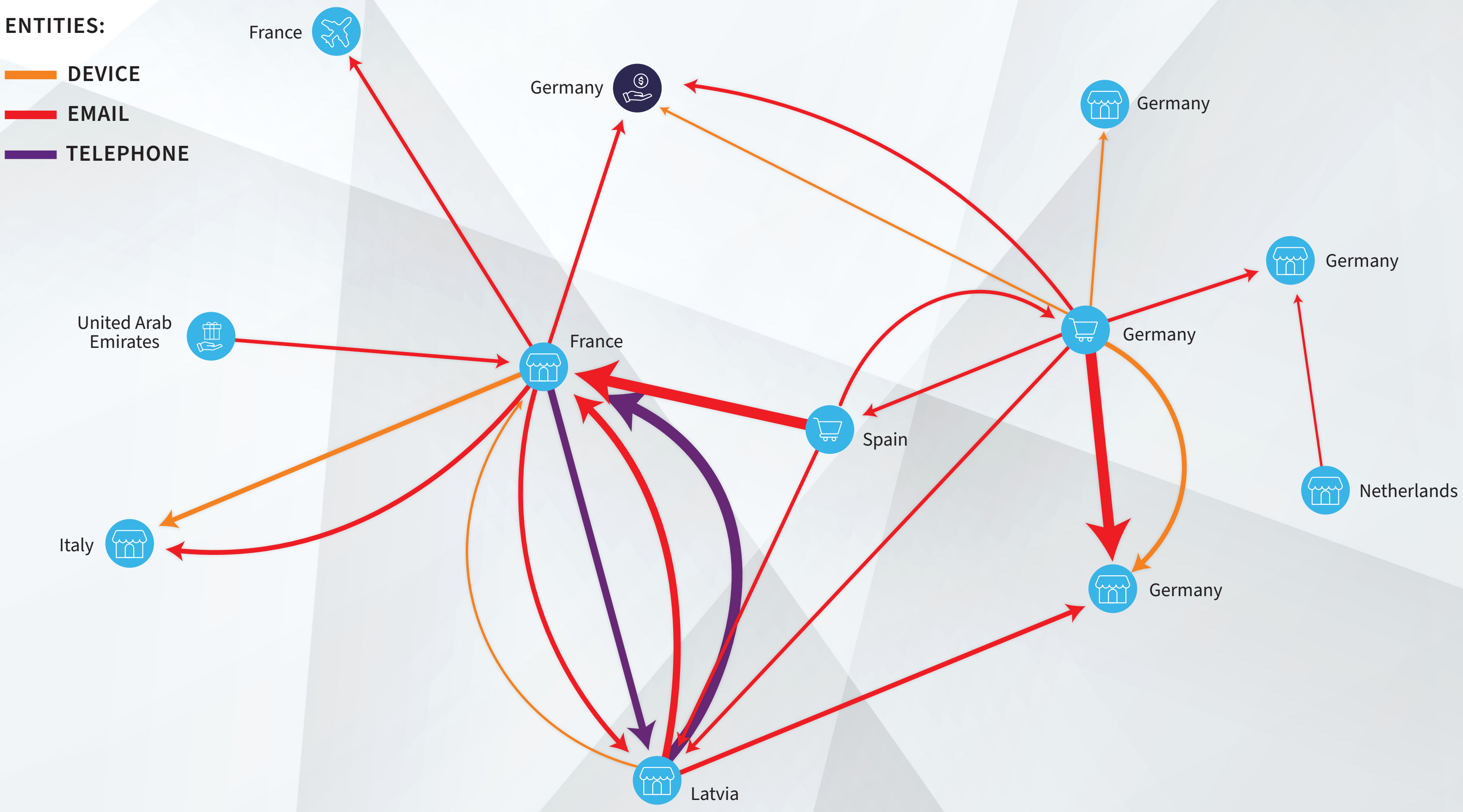
Events recorded at other organizations in the Digital Identity Network that were associated with either a device, email address and/or telephone number that was involved in these original fraudulent events at source organizations.

At least $250K

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

See next page for fraud network visualization

SHARED STOLEN CREDENTIALS USED BY GROUPS OF CYBERCRIMINALS FOR ACCOUNT TAKEOVER AND FRAUDULENT PAYMENTS



ENTITIES:

- ▬ DEVICE
- ▬ EMAIL
- ▬ TELEPHONE

FINANCIAL SERVICES:

- PAYMENT GATEWAY

ECOMMERCE:

- MARKETPLACE
- LOYALTY PROGRAM
- RETAILER
- TRAVEL

This fraud network only shows connections of more than 10 entities. A thicker line denotes a higher volume of fraud.

SPOTLIGHT: ANALYZING THE IMPACT OF BREACHED EMAIL ADDRESSES ACROSS THE DIGITAL IDENTITY NETWORK

FRAUD:
Identity testing attacks across multiple organizations in the Digital Identity Network using apparently stolen email addresses. Most of the email domains are genuine (gmail.com, hotmail.com, yahoo.com), indicating that these emails are likely stolen from genuine consumers rather than synthetically created.

TARGET:
A gaming and gambling operator, a retailer and an airline.

METHOD:
Large volume bot attacks testing multiple email addresses during short, sustained attacks.

ATTACK:

- **Airline** 13,000 account takeover attempts linked to 3,200 stolen emails.
- **Gaming and gambling operator** Over 2,500 account takeover attempts linked to 10 stolen emails also seen in attack at airline.
- **Retailer** 1,150 account takeover attempts linked to over 800 stolen emails, one of which is also seen at the airline.
- Emails continue to be used by genuine customers at other organizations in the Digital Identity Network.

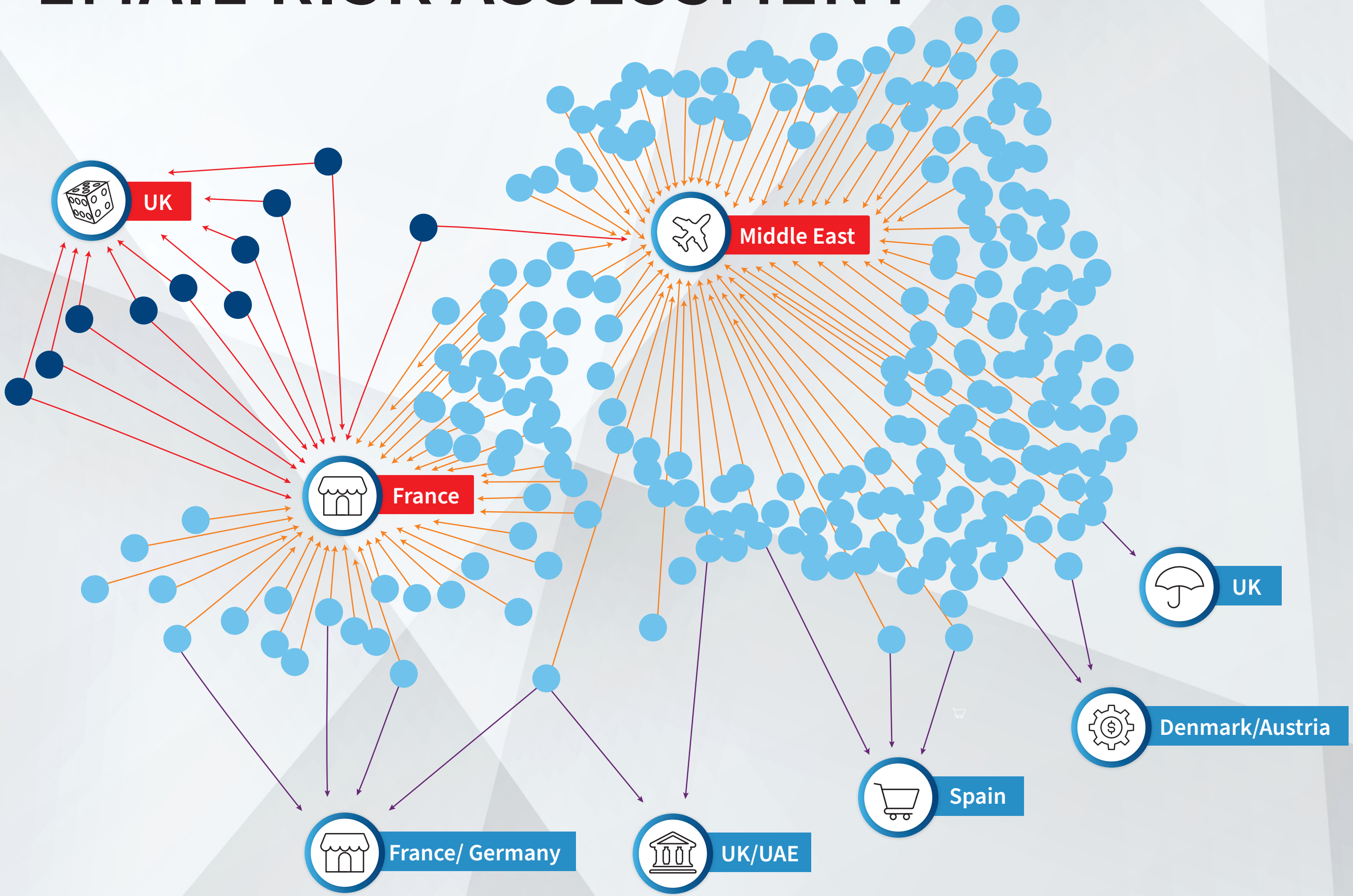
DETECTION:
Email risk assessment from the Digital Identity Network differentiates between legitimate and fraudulent use of email addresses.

USE OF STOLEN EMAIL ADDRESSES ACROSS ORGANIZATIONS HIGHLIGHTS THE IMPORTANCE OF ROBUST EMAIL RISK ASSESSMENT

Stolen email address used in attacks **across organizations**

Stolen email address used in attack at **one organization**

Email address **used by genuine customer at other organizations**



GAMING AND GAMBLING OPERATOR

AIRLINE

RETAILER

BANK

MARKETPLACE

FINTECH

INSURANCE

SPOTLIGHT: ANALYZING NETWORKED FRAUD ATTACKS LINKED BY DIFFERENT PIECES OF DIGITAL IDENTITY DATA

Uniting All Elements of Digital Identity Data Reveals Previously Unseen High-Risk Connections

Fraud Attack

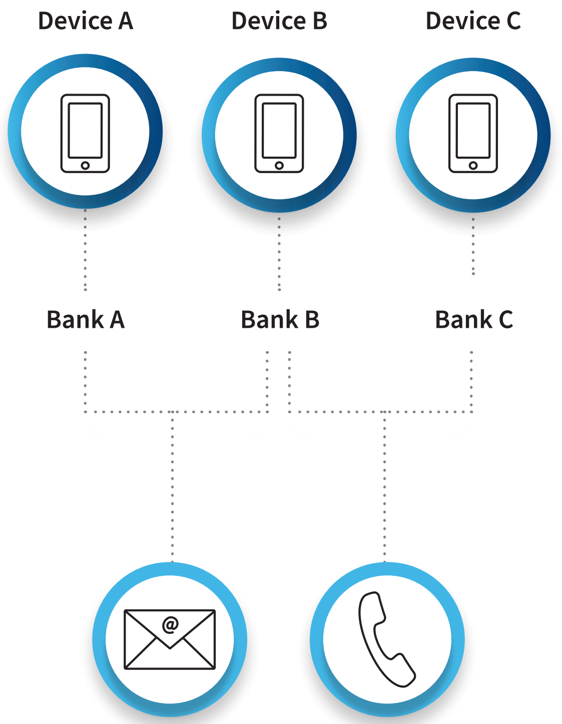
Fraudster using 3 different devices at 3 different banks.

3 fraudulent transactions cannot be linked as there is no common identifier.

Adding in Additional Data

Links Device A and B by an email address.

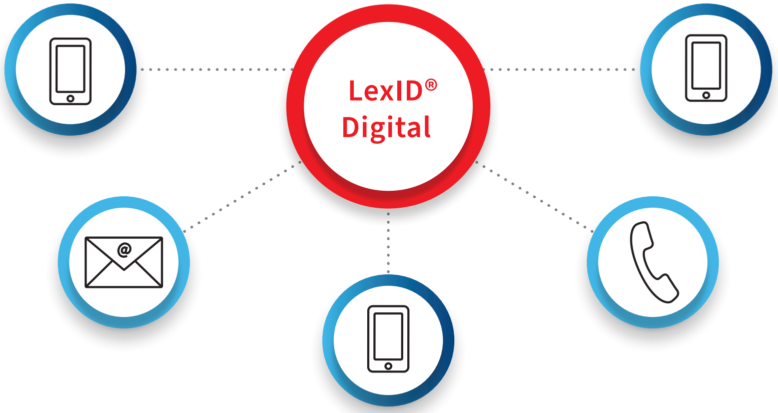
Links Device B and C by telephone number.



Building This Digital Identity in the Digital Identity Network

An online digital identity can be built in the Digital Identity Network by linking the 3 fraudulent transactions via the email address and telephone number.

When any of these individual entities is seen in a new transaction, the history of the digital identity can be checked for fraud.



03

THE CYBERCRIME LANDSCAPE:

JULY-DECEMBER 2020

ACROSS THE CUSTOMER JOURNEY

CUSTOMER JOURNEY HIGHLIGHTS: JULY-DECEMBER 2020

NEW ACCOUNT CREATIONS

- Highest attack rate of all use cases.
- 1 in every 10 transactions in the Digital Identity Network is an attempted attack.

LOGINS

- Low overall attack rate.
- 9% growth in percentage of mobile attacks YOY.

PAYMENTS

- Significant growth in payment transaction volume YOY, as consumers rely on digital payment methods more than ever before.
- Higher volume of attempted attacks on payment transactions than any other use case.

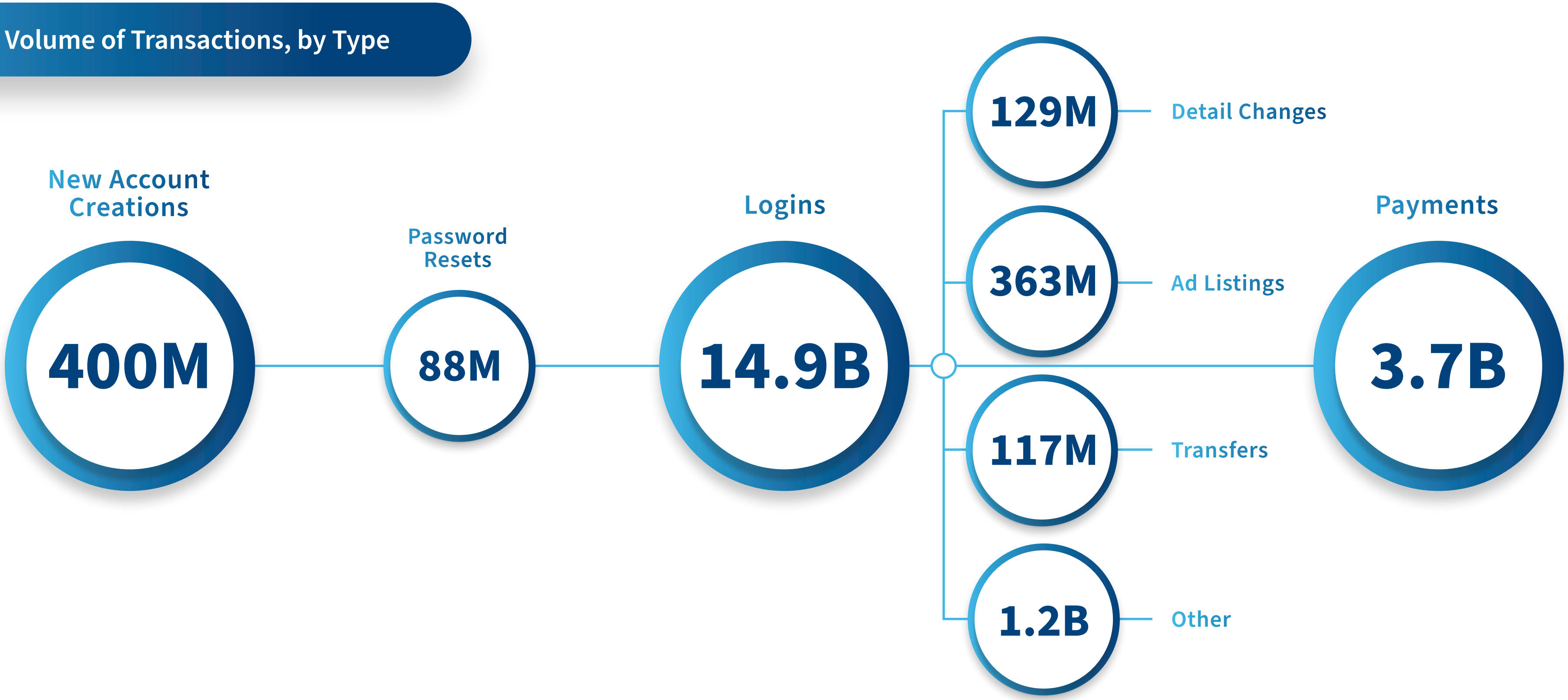
DETAILS CHANGE

- Of the non-core use cases, change in details transactions see the highest rate of attack at 2.2%.

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.

ATTACK RISKS ACROSS CORE TOUCHPOINTS

Decline in Attack Rates Across All Use Cases July to December 2020

	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	The volume of attacks has decreased significantly YOY. This is due to a huge bot attack targeting new account creations in financial services between Dec. 2019 and Jan. 2020 which dramatically increased attack volumes. Comparatively, H2 2020 attack volumes are low.	Login transactions continue to experience low overall attack rates due to a high volume of transactions from trusted and returning customers. However, the absolute number of attacks is significant, illustrating the potential risk to good user accounts.	Payment transactions see the highest volume of attacks across all use cases, with mobile browser transactions experiencing the highest attack rate.
ATTACK VOLUME	39M	62M	108M
ATTACK RATE			
⚠ OVERALL	9.8%	0.4%	2.9%
DESKTOP	**13.9%**	**0.8%**	3.3%
MOBILE BROWSER	9.1%	0.7%	**3.4%**
MOBILE APP	5.4%	0.1%	1.7%

H2 refers to the July to December period.

ATTACK RISKS ACROSS ADDITIONAL HIGH-RISK TOUCHPOINTS

Details Change Transactions Can Present High-Risk Precursor to Future Attacks

	PASSWORD RESETS	DETAILS CHANGES	AD LISTINGS	TRANSFERS	OTHER
RISK TRENDS	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 (OTP) authentication checks, are sent to the fraudster. Large attacks targeting details change transactions within financial services contributed to the high mobile app attack rate during this period.	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	0.7M	2.9M	1.8M	1.1M	19.3M
ATTACK RATE					
OVERALL	0.8%	2.2%	0.5%	0.9%	1.6%
DESKTOP	**0.9%**	1.2%	0.5%	**1.8%**	**2.2%**
MOBILE BROWSER	**0.9%**	1.3%	**1.5%**	1.2%	1.2%
MOBILE APP	0.2%	**3.8%**	0.4%	0.6%	1.2%

04

THE CYBERCRIME LANDSCAPE: JULY-DECEMBER 2020 REGIONAL TRENDS

REGIONAL HIGHLIGHTS: JULY-DECEMBER 2020

APAC

▲ **+24%** **growth** in transaction volume YOY.

▼ **-42%** **decline** in human-initiated attacks YOY.

▼ **-2%** **decline** in bot volume YOY.

EMEA

▲ **+23%** **growth** in transaction volume YOY.

▼ **-54%** **decline** in human-initiated attacks YOY.

▼ **-6%** **decline** in bot volume YOY.

LATAM

▲ **+18%** **growth** in transaction volume YOY with a 16% growth in mobile transaction penetration – the highest of all regions.

▼ **-26%** **decline** in human-initiated attacks YOY.

▼ **-20%** **decline** in bot volume YOY.

NORTH AMERICA

▲ **+37%** **growth** in transaction volume YOY.

▼ **-37%** **decline** in human-initiated attacks YOY.

▲ **+1%** **growth** in bot volume YOY.

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

IDENTITY ABUSE INDEX BY REGION

LATAM and APAC Experience Most Volatile Attack Rates

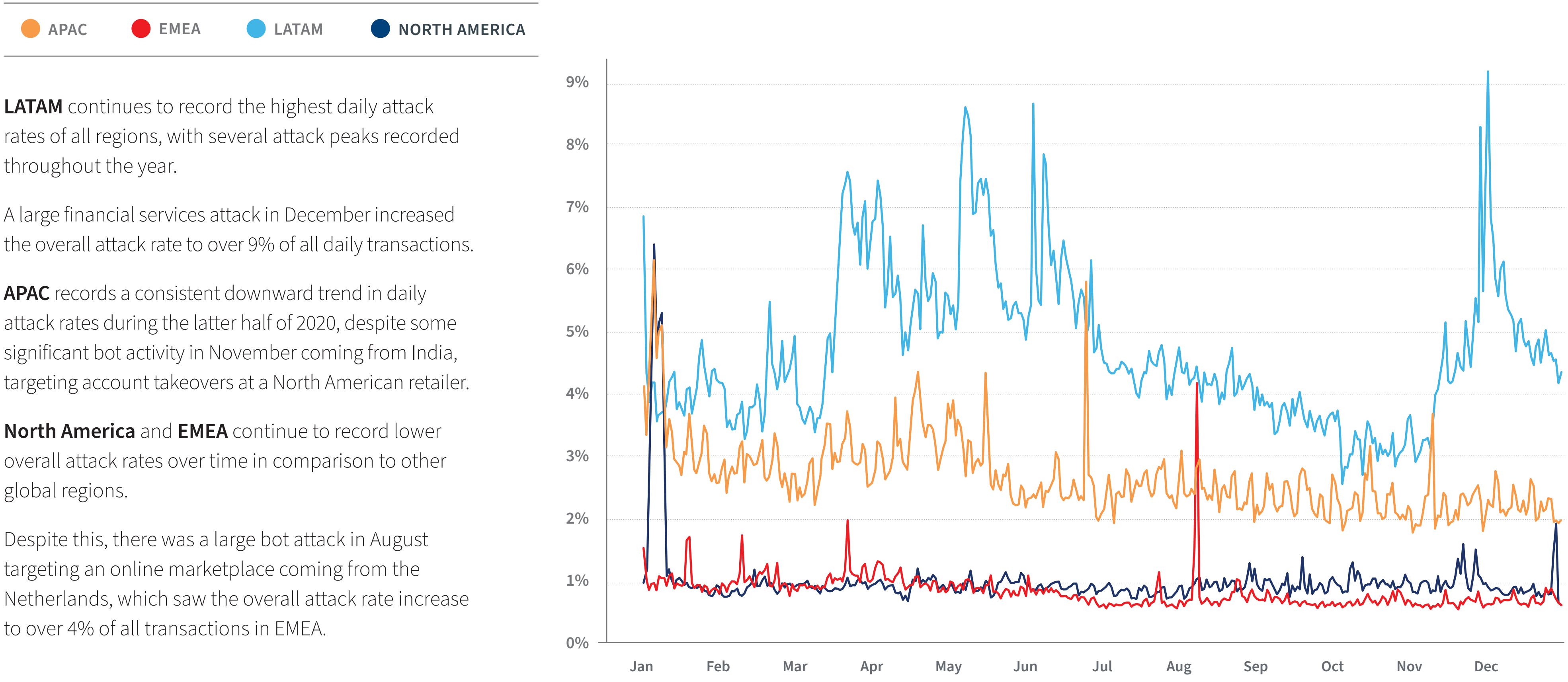
LATAM continues to record the highest daily attack rates of all regions, with several attack peaks recorded throughout the year.

A large financial services attack in December increased the overall attack rate to over 9% of all daily transactions.

APAC records a consistent downward trend in daily attack rates during the latter half of 2020, despite some significant bot activity in November coming from India, targeting account takeovers at a North American retailer.

North America and **EMEA** continue to record lower overall attack rates over time in comparison to other global regions.

Despite this, there was a large bot attack in August targeting an online marketplace coming from the Netherlands, which saw the overall attack rate increase to over 4% of all transactions in EMEA.



APAC TRANSACTION AND ATTACK PATTERNS

APAC

TOP 5 ATTACKERS

1. India
2. Japan
3. Bangladesh
4. Philippines
5. Malaysia

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. UK
3. Australia
4. Japan
5. Malaysia

TRANSACTIONS

TRANSACTIONS PROCESSED

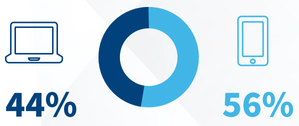
1.7B

Growth YOY

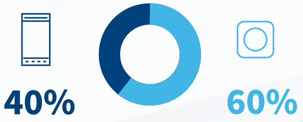
+24% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

33M

Decline YOY

-42% ▼

AUTOMATED BOT ATTACK VOLUME

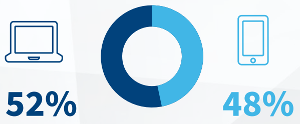
142M

Decline YOY

-2% ▼

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



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

-15% ▼

APAC

APAC POSITION AGAINST GLOBAL FIGURES

APAC Sees Higher Attack Rates Across All Channels in Comparison to Global Figures

🌐 GLOBAL 📍 APAC

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

The APAC region remains a large contributor to global bot attacks, with Japan, India and Australia all appearing on the list of top attack originators globally.

The volume of automated bot attacks coming from the APAC region is largely consistent YOY.

OVERALL ATTACK RATE

🌐 1.1% 📍 2.3%

DESKTOP ATTACK RATE

🌐 1.6% 📍 2.8%

MOBILE BROWSER ATTACK RATE

🌐 2.3% 📍 3.0%

MOBILE APP ATTACK RATE

🌐 0.4% 📍 1.3%

EMEA TRANSACTION AND ATTACK PATTERNS

EMEA

TOP 5 ATTACKERS

1. UK
2. Germany
3. Saudi Arabia
4. Netherlands
5. Russia

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. UK
3. Canada
4. Russia
5. Sweden

TRANSACTIONS

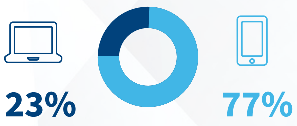
TRANSACTIONS PROCESSED

8.7B

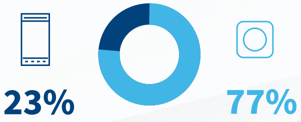
Growth YOY +23% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

60M

Decline YOY -54% ▼

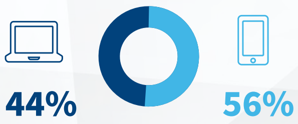
AUTOMATED BOT ATTACK VOLUME

256M

Decline YOY -6% ▼

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



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

-13% ▼

EMEA

EMEA POSITION AGAINST GLOBAL FIGURES

EMEA has Highest Penetration of Mobile App Transactions of any Global Region

🌐 **GLOBAL** 📍 **EMEA**

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

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

Despite this, however, several EMEA countries feature on the lists of largest contributors to both human-initiated and bot attacks, by volume.

OVERALL ATTACK RATE

🌐 1.1% 📍 0.8%

DESKTOP ATTACK RATE

🌐 1.6% 📍 1.4%

MOBILE BROWSER ATTACK RATE

🌐 2.3% 📍 1.8%

MOBILE APP ATTACK RATE

🌐 0.4% 📍 0.2%

LATAM TRANSACTION AND ATTACK PATTERNS

LATAM

TOP 5 ATTACKERS

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

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. Brazil
3. UK
4. Chile
5. Mexico

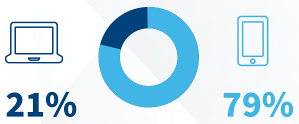
TRANSACTIONS

TRANSACTIONS PROCESSED

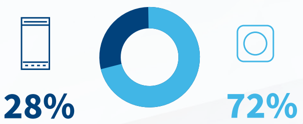
875M — Growth YOY +18% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

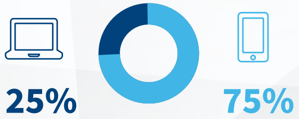
33M — Decline YOY -26% ▼

AUTOMATED BOT ATTACK VOLUME

44M — Decline YOY -20% ▼

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



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

+2% ▲

LATAM POSITION AGAINST GLOBAL FIGURES

Attack Rates Across All Channels Higher Than Any Other Global Region

🌐 GLOBAL 📍 LATAM

Although overall attack rates in LATAM have fallen YOY, they remain the highest of all global regions, particularly for mobile app transactions.

Automated bot volume also fell 20% YOY. Brazil is the only country in LATAM to appear on the list of largest bot originators.

The percentage of mobile transactions in LATAM has grown 16% YOY, suggesting that mobile is perhaps facilitating financial inclusion in the region. LATAM has now overtaken EMEA as the region with the highest penetration of mobile transactions, with nearly 4 in every 5 transactions coming from a mobile device.

	🌐 GLOBAL	📍 LATAM
OVERALL ATTACK RATE	1.1%	4.1%
DESKTOP ATTACK RATE	1.6%	5.0%
MOBILE BROWSER ATTACK RATE	2.3%	5.9%
MOBILE APP ATTACK RATE	0.4%	3.2%

NORTH AMERICA TRANSACTION AND ATTACK PATTERNS

TOP ATTACKERS

1. U.S.
2. Canada

TOP 5 ATTACK DESTINATIONS

1. U.S.
2. Canada
3. Australia
4. UK
5. Brazil

TRANSACTIONS

TRANSACTIONS PROCESSED

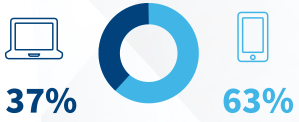
12.6B

Growth YOY

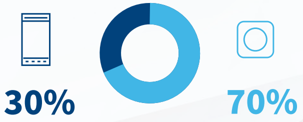
+37% ▲

TRANSACTIONS SPLIT BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



ATTACKS

HUMAN-INITIATED ATTACK VOLUME

105M

Decline YOY

-37% ▼

AUTOMATED BOT ATTACK VOLUME

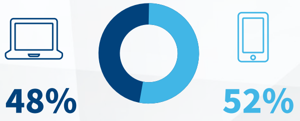
747M

Growth YOY

+1% ▲

ATTACKS SPLIT BY CHANNEL

Desktop / Mobile



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

-24% ▼

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

NORTH AMERICA

NORTH AMERICA POSITION AGAINST GLOBAL FIGURES

Large Growth in Automated Bot Volume July-December 2020

🌐 GLOBAL 📍 NORTH AMERICA

North America continues to experience low overall attack rates in comparison to the global averages, following a similar pattern to the EMEA region.

The human-initiated attack rate has also declined in this region, while the bot attack volume has remained largely consistent, with a 1% increase recorded YOY.

Nevertheless, the U.S. is the top originator of both human-initiated and bot attacks by volume, while Canada consistently appears in a top 3 position.

	🌐	📍
OVERALL ATTACK RATE	1.1%	1.0%
DESKTOP ATTACK RATE	1.6%	1.3%
MOBILE BROWSER ATTACK RATE	2.3%	2.2%
MOBILE APP ATTACK RATE	0.4%	0.2%

05

THE CYBERCRIME LANDSCAPE:

JULY-DECEMBER 2020

INDUSTRY OPPPORTUNITIES

INDUSTRY HIGHLIGHTS: JULY-DECEMBER 2020

FINANCIAL SERVICES

- Low overall attack rates, driven by a high volume of repeat login transactions from trusted customers.
- The exception is for payment transactions, which are attacked at a higher rate than any other industry, presenting a key opportunity for fraudsters to cash out.
- Growth in attacks targeting new account creations from desktops and mobile browsers.

ECOMMERCE

- eCommerce experienced the largest growth in bot volume in comparison to other industries, despite declining human-initiated attack rates.
- The attack rate for eCommerce payments made on a mobile app is higher than for any other industry, representing a potential point of risk.

MEDIA

- New account creations attacked at a higher rate than any other industry, with fraudsters using media organizations to test stolen identity data.
- Growth in attack rates across new account creations from desktops and mobile browsers, as well as login transactions from both mobile browsers and mobile apps.

INDUSTRY OVERVIEW: TRENDS AND ATTACK PATTERNS

The Media Industry Experiences the Highest Attack Rates Across All Use Cases, While Desktop Transactions Are the Most Targeted of All Channels

INDUSTRY OVERVIEW	ALL INDUSTRY SUMMARY	FINANCIAL SERVICES	ECOMMERCE	MEDIA
RISK TRENDS	Desktop transactions attacked at the highest rate of all channels.	Despite high attack volumes, overall attack rates are the lowest of all industries driven by large volumes of repeat, trusted transactions.	The mobile app attack rate (a subset of the mobile attack rate) on payment transactions is higher for eCommerce merchants than any other industry.	New account creations represent the biggest risk in the media customer journey, both in terms of attack volumes and attack rates.
ATTACK VOLUME	235M	123M	65M	46M
ATTACK RATE				
OVERALL	1.1%	0.8%	1.4%	**4.5%**
DESKTOP	**1.6%**	**1.3%**	**1.8%**	**4.2%**
MOBILE	0.9%	0.7%	1.1%	**4.7%**

FINANCIAL SERVICES: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Financial Services Payments Transactions Record Highest Attack Rate of All Industries

FINANCIAL SERVICE OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Significant drop in attack volume/ mobile app attack rate due to large bot attack targeting mobile app new account creations in December 2019/January 2020 which led to a huge peak in attacks during this period. However, growth was recorded in attack rates across desktop and mobile browser transactions.	The overall attack rate on login transactions remains low due to a high volume of regular transactions from trusted customers. However, the 36 million attempted account takeovers represent a significant risk to good customer accounts. Desktop and mobile browser transactions are attacked at the highest rate, although attack rates fell YOY.	As the volume of payment transactions has increased YOY, so too has the volume of attacks. However, the attack volume growth was less pronounced than the transaction volume growth, leading to an overall decline in attack rates.
ATTACK VOLUME	5M (94M)	36M (48M)	69M (58M)
ATTACK RATE OVERALL	4.1% (18.3%)	0.3% (0.5%)	3.6% (4.5%)
DESKTOP	**7.1%** (5.0%)	**0.7% (1.2%)**	4.1% (4.2%)
MOBILE BROWSER	3.4% (3.1%)	**0.7%** (1.0%)	**4.9% (6.3%)**
MOBILE APP	2.3% **(20.8%)**	0.1% (0.2%)	1.0% (2.2%)

Numbers in brackets are H2 2019 figures.

ECOMMERCE: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Overall Decline in Attack Rates Punctuated by 32% Growth in Bot Volume YOY

ECOMMERCE OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	New account creations from a desktop continue to be attacked at a higher rate than any other use case, with more than one in every 10 transactions identified as a potential attack. Despite this, however, the attack rates are declining across all channels.	Although eCommerce merchants experience a higher rate of account takeover attempts in comparison to financial services, overall attack rates remain relatively low, and are declining across all channels YOY.	Payment transactions in the eCommerce customer journey represent a significant opportunity for fraudsters to cash out and monetize stolen credentials. Although the attack rates are also declining across all channels, the mobile app attack rate is higher for eCommerce merchants than any other industry.
ATTACK VOLUME	6M (8M)	19M (49M)	36M (44M)
ATTACK RATE			
OVERALL	5.2% (11.3%)	1.0% (3.4%)	2.3% (3.8%)
DESKTOP	**10.7% (25.9%)**	**1.3%** (3.3%)	**2.7% (4.7%)**
MOBILE BROWSER	2.7% (4.5%)	0.8% (2.9%)	1.6% (2.9%)
MOBILE APP	1.3% (4.0%)	0.2% **(4.3%)**	**2.7%** (3.8%)

Numbers in brackets are H2 2019 figures.

MEDIA: OVERVIEW OF TRENDS AND ATTACK PATTERNS

Media New Account Creations Record Significantly Higher Attack Rates than Any Other Industry

MEDIA OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
RISK TRENDS	Around 1 in every 6 new account creation transactions is a potential attack, with a growth in attack rates recorded across desktop and mobile browser. It's likely that many of these new account creation attempts comes from fraudsters testing stolen identity data on companies which typically have lower barriers to entry. Attempts are made to abuse new customer bonuses, or to resell trial periods for financial gain.	The overall login attack rate is comparable to eCommerce. Media organizations, however, have seen a growth in the mobile browser and mobile app attack rate YOY.	Attack rates on media payments are lower than in other industries, likely because they represent less opportunity to "cash out" in comparison to an eCommerce or financial services payment. However, the industry recorded a significant growth in bots making payment transactions YOY. These are likely fraudsters testing stolen credit card data before using validated cards in a more lucrative attack elsewhere.
ATTACK VOLUME	29M (30M)	7M (9M)	3M (3M)
ATTACK RATE			
⚠ OVERALL	16.6% (15.5%)	1.1% (1.9%)	1.8% (2.5%)
DESKTOP	**21.9%** (18.3%)	0.7% **(2.8%)**	**2.0% (2.9%)**
MOBILE BROWSER	14.9% (12.1%)	0.8% (0.6%)	1.9% (2.8%)
MOBILE APP	15.7% **(25.4%)**	**5.1%** (0.8%)	1.1% (1.5%)

Numbers in brackets are H2 2019 figures.

LexisNexis® RISK SOLUTIONS

GAMING AND GAMBLING (SUBSET OF MEDIA): OVERVIEW OF TRENDS AND ATTACK PATTERNS

Bonus Abuse and Account Takeover Opportunities Attract Fraudsters to Global Gaming and Gambling Operators

GAMING AND GAMBLING OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK RATE			
⚠ OVERALL	9.4%	0.9%	0.8%
DESKTOP	**12.6%**	**1.3%**	0.7%
MOBILE BROWSER	9.0%	0.9%	**1.0%**
MOBILE APP	3.6%	0.1%	0.3%

- New player bonuses make gaming and gambling operators susceptible to multiple fraudulent new account creations. Fraudsters often exploit free gaming opportunities on a mass scale, thereby increasing their chances of winning the jackpot.
- This accounts for the high attack rate on new account creations, particularly on desktop transactions.
- While the attack rate on account logins remains low, the significant volume of attempted account takeovers represents the risk posed to the industry by fraudsters looking to access good user account balances, or simply to launder proceeds of crime across different industries and geographies.

TELCO (SUBSET OF MEDIA): OVERVIEW OF TRENDS AND ATTACK PATTERNS

Telco Organizations Risk Large Monetary Exposure from Fraudulent New Account Creations and Account Takeovers

TELCO OVERVIEW	NEW ACCOUNT CREATIONS	LOGINS	PAYMENTS
ATTACK RATE			
⚠ OVERALL	1.1%	0.2%	1.9%
DESKTOP	1.0%	**0.3%**	1.8%
MOBILE BROWSER	**1.1%**	0.1%	**2.0%**

- Telco organizations offer fraudsters the opportunity to launder high-value hardware, as well as register pre and post-paid mobile phone contracts to commit further fraud.
- With the shift from physical stores to digital transacting further accelerated because of COVID-related lockdowns, telco organizations have had to prioritize their digital transformation, moving away from in-person selling and KYC checks that were typical of the in-store experience.
- Although overall attack rates remain low, monetary exposure from individual new account creations and account takeovers can be extremely high. This is largely due to the high value of mobile phones and the potential to quickly build up large account charges, particularly on content downloads and media streaming.

Mobile app data has been excluded due to low volumes of transactions.

06

CYBERCRIME IN A PANDEMIC: CONSUMER TRENDS AND FRAUD TYPOLOGIES

SUMMARY:

- While specific fraud typologies have proliferated during the global pandemic, overall attack rates in the Digital Identity Network have fallen.
- Automation and identity spoofing remain key attack vectors during 2020.
- With many new-to-digital customers coming online for the first time, the youngest age group – under 25s – are most susceptible to fraud attacks.
- However, the oldest age group sees the next highest rate of attack, making them similarly vulnerable.
- Fraud losses increase progressively with age, making the older population most at risk of suffering the largest fraud losses.

CYBERCRIME IN A PANDEMIC

A Summary of Consumer Trends and Fraud Typologies During 2020

CONSUMER TRENDS

34% growth in online payments YOY.

26% growth in login transactions YOY.

Growth in transaction volumes coming from new devices and new digital identities, as well as existing customer transacting more.

Fall in overall attack rates indicates a higher proportion of transactions from trusted customers.

Growth in new online banking customers registering for web and mobile services.

Less login activity from consumers who had traveled more than 1,000km (621 miles) in a week, as well as a shift in logins from metropolitan to suburban areas.

FRAUD TYPOLOGIES

Identity spoofing was the most prevalent attack vector and was seen in 5% of all global transactions. This was followed by device spoofing at 4.2%.

Attack growth generally comes from automated bot volume, indicating automation is method of choice for current attacks.

Media remains the industry with the highest overall attack rates, although financial services see the highest attack rate on payments.

Fraud recorded against government stimulus packages, across multiple banks, e.g., targeting the Bounce Back Loan Scheme in the UK.

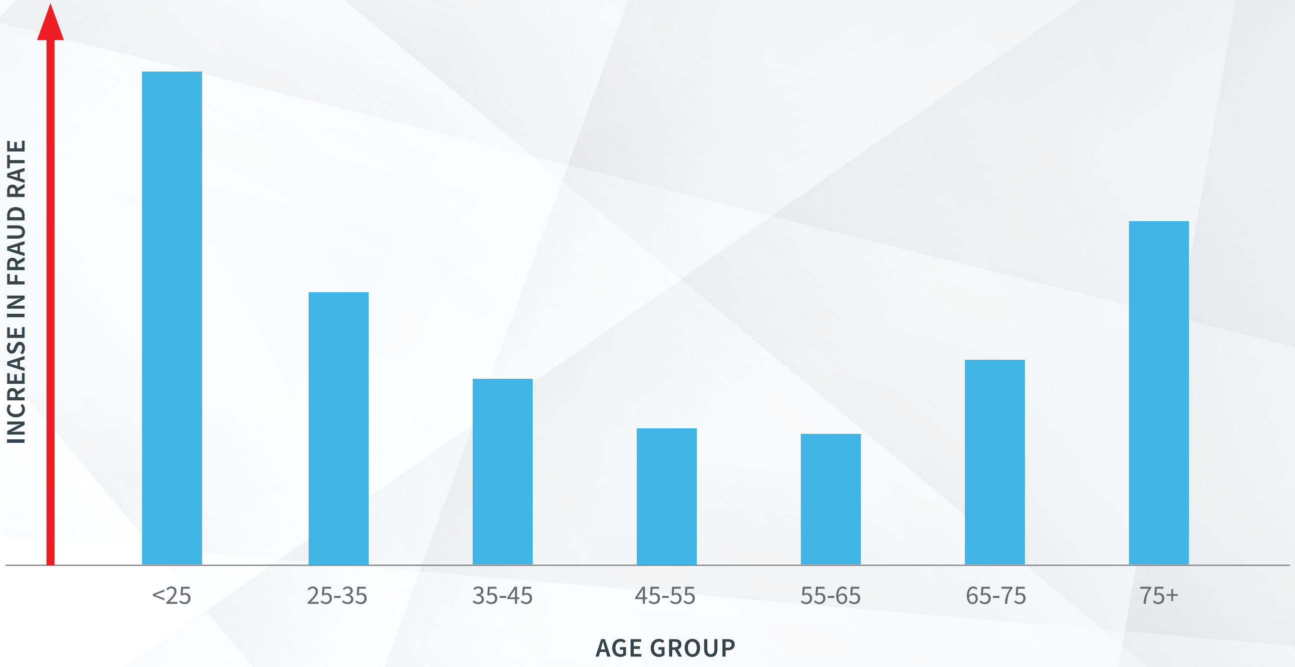
Early indications that consumers are feeling economic pressure with growth in first-party chargeback fraud rate across eCommerce.

FRAUD RISK BY AGE: WHICH CUSTOMERS ARE MOST VULNERABLE TO FRAUD ATTACKS?

With New-to-Digital Customers Coming Online in Larger Numbers, Are They at Greater Risk?

- The largest growth in new customers coming online in 2020 was in the under 25 age group, with a 10% growth recorded across a four-month period.
- Analysis shows that this age group is also most vulnerable to fraud attacks, followed closely by the over 75 age group.
- News reports often suggest that millennials are fairly relaxed about sharing data online, making them more exposed to potential data breaches or identity theft.
- The over 75 age group, sometimes referred to as the silent generation, generally has less familiarity with the latest digital technologies and may therefore be more susceptible to scams and phishing attempts.

FRAUD RATE BY AGE

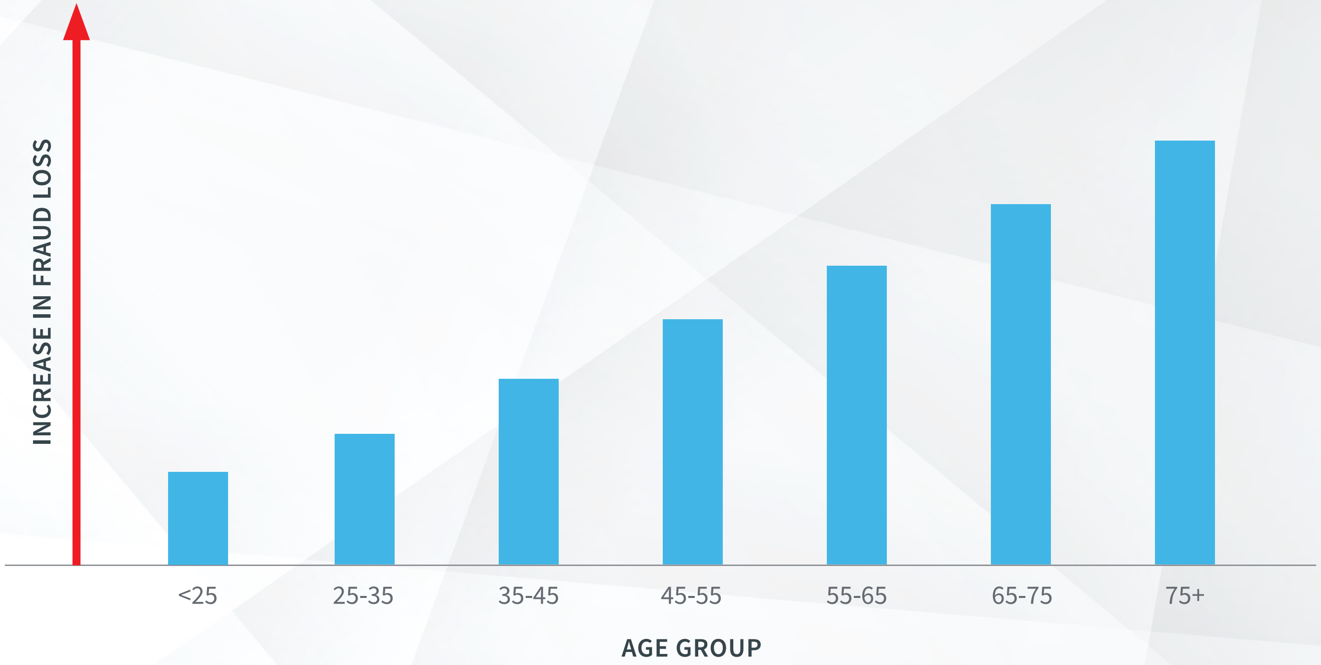


FRAUD RISK BY AGE: WHICH CUSTOMERS LOSE THE MOST MONEY IN FRAUD ATTACKS?

How Can Organizations Protect Those at Greatest Risk of Losing Most?

- While millennials and zillennials are most susceptible to fraud attacks, the average fraud loss per customer increases progressively with age, likely influenced by larger disposable incomes later in life.
- The paradox of why fraudsters choose to target the younger age group in proportionally higher volumes can perhaps be answered by the fact that higher success rates can offset the lower monetary gains.
- Protection of the older, and potentially more vulnerable population, is critical for organizations that are prioritizing a digital-first strategy.
- Businesses must educate customers as to the modus operandi of fraud attacks, while ensuring that the online customer journey protects against attacks, with relevant and timely online messaging as appropriate.

AVERAGE FRAUD LOSS PER CUSTOMER



07 CONCLUSION

PREDICTIONS FOR THE YEAR AHEAD: THE OPPORTUNITY FOR DIGITAL BUSINESSES

With change, huge opportunity often emerges. This opportunity, however, presents itself not just to forward-thinking digital businesses, but also to cybercriminals who can remain just ahead of the technology curve. As organizations continue to merge their digital and physical services, innovating to meet an increasingly diverse consumer base, fraud prevention strategies must keep pace with this evolution, transformation and growth. Without a robust, and layered approach, businesses are opening themselves up to new fraud risks. Fraudsters remain masters of disguise, continually searching out the weakest link under a cloak of legitimacy.

Market-leading innovation will continue apace to facilitate this complex set of opportunities and mitigate associated risks for global digital businesses. At its core, this should provide businesses with the ability to layer digital and physical identity and authentication solutions across an omni-channel customer journey.

This weakest link may well be those new-to-digital customers who have come online during the pandemic. Younger adults and the older population have been shown to be the most susceptible to fraud attacks. Fraud prevention extends not only to detecting identity spoofing, automated bot attacks and account takeovers, but also to awareness, education and customer messaging that shows all customers how to better spot potential scams. It's likely that we will continue to see fraudsters preying on pandemic-related anxieties, offering investments that look too good to be true or products that are in hot demand online.

It's not just new customers that must be protected, however. Trusted, existing customers may be inconvenienced with additional authentication steps as "back to normal" behavior is potentially flagged as unusual following the unprecedented change that took place in consumer behavior in 2020. How can organizations ensure that reliable fraud prevention does not mean unnecessary friction for good customers?

Regulatory change and economic uncertainty will also merge with this evolving digital landscape:

Open banking platforms will become a key target for fraudsters looking to exploit customer data across accounts. PSD2 in Europe will see fraudsters looking for loopholes and exemptions in tighter fraud defenses. Again, good customers may see a change to transaction acceptance rates with the new swath of authentication strategies that mandate two layers of strong customer authentication (SCA).

It's likely too that as economies respond to the impact of the pandemic, fraudsters will look to benefit from the downturn via increased mule recruitment, promising consumers fast money in return for use of their bank account to funnel proceeds of crime through global organizations.

eCommerce merchants will likely see a growth in first-party fraud as more consumers feel the economic pinch.

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.

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

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

Common Attacks

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

Account Login Fraud: Attacks targeted at taking over user accounts using previously stolen credentials available in the wild or credentials compromised by malware or Man-in-the-Middle attacks.

Payment Fraud: Using stolen payment credentials to conduct illegal money transfers or online payments via alternative online payment methods such as direct deposit.

Percentages

Transaction Type Percentages are based on the number of transactions (account creations, account login and payments) from mobile devices and desktop computers received and processed by the Digital Identity Network.

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

Desktop Versus Mobile

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

Desktop Attacks are attacks that target a transaction originating from a desktop device.

Mobile Transactions are transactions that originate from a handheld mobile device such as tablet or mobile phone. These include mobile browser and mobile app transactions.

Mobile Attacks are attacks that target transactions originating from a mobile device, whether browser or app-based.

Attack Explanations

Device Spoofing: Fraudsters delete and change browser settings in order to change their device identity or fingerprint, or attempt to appear to come from a victim's device. LexisNexis® ThreatMetrix® patented cookieless device identification is able to detect returning visitors even when cookies are deleted or changes are made to browser settings. To differentiate between cybercriminals and legitimate customers who occasionally clear cookies, only high-risk / high velocity cookie deletions (such as a high number of repeat visits per hour / day) are included in the analysis.

Identity Spoofing: Using a stolen identity, credit card or compromised username/password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on a high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user accounts or unusual identity linkages and usage.

IP Address Spoofing: Cybercriminals use proxies to bypass traditional IP geolocation filters, and use IP spoofing techniques to evade velocity filters and blacklists. LexisNexis ThreatMetrix® directly detects IP spoofing via both active and passive browser and network packet fingerprinting techniques.

Man-in-the-Browser (MitB) and Bot Detection: Man-in-the-browser attacks use sophisticated Trojans to steal login information and one-time-passwords from a user's browser. Bots are automated scripts that attempt to gain access to accounts with stolen credentials or create fake accounts.

LexID® Digital

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

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

SUMMARY METHODOLOGY

Overall Report

- The LexisNexis Risk Solutions Cybercrime Report is based on cybercrime attacks detected by the LexisNexis Digital Identity Network (the Digital Identity Network) from July – December 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 July to September 2020, based upon devices, email addresses and telephone numbers recorded as fraudulent in the Digital Identity Network.
- Monetary exposure calculated on observed payment transactional value at risk July to September 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.

DATA PROCESSED AND ANALYZED

The overall volume of transactions processed by the Digital Identity Network July – December 2020 was 28.4 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 24.6 billion transactions.

The Cybercrime Report uses these 24.6 billion transactions to calculate overall transaction volumes globally and by region. There are 880K 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 24.6 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 20.9 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.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis® does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis.

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