LexisNexis®
RISK SOLUTIONS

LEXISNEXIS® RISK SOLUTIONS CYBERCRIME REPORT

Global Insights from the LexisNexis® Digital Identity Network®

January-June 2019

Foreword

The human / robot dichotomy is one that permeates evolutionary rhetoric the world over, with global digital businesses faced with a rapidly evolving challenge to reliably distinguish between the customers they want to interact with, and fraudsters who are attempting to destabilize their brand, reputation and bottom line.

- **In technology, the research company OpenAI has developed Artificial Intelligence that is so advanced at writing text that the company has made the decision to keep the model under wraps for fear that it could be exploited to create fake news as "real" as genuine articles.**

- **In robotics, humanoid robots are being programmed not only to walk and talk like real people, but to express emotions; perhaps the final bastion of what it means to be human.**

- **In biometrics, an engineering team from NYU has already succeeded in developing a synthesized human fingerprint, until now the very essence of what makes people unique and impossible to replicate. Early indications suggest that this fake fingerprint could potentially fool touch-based authentication systems.**

It's clear that the distinguishing features of what constitutes humanity are being continually challenged and stretched by a rapidly advancing technological landscape. This phenomenon is further playing out in vivid technicolor in the fraud and identity space. Identity, in its most fundamental form, is being constantly challenged; whether by synthetic identity creation, the permeation of stolen identity data, the mimicking of good customer behavior or the attack of automated bots that behave like human traffic.

Point solutions are being targeted and breached at every turn, as evidenced by the creation of fake fingerprints and human-like bot attacks. When attacks on accounts or networks fail, fraudsters often resort to the path of least resistance - consumers themselves. Consumers are unwittingly becoming involved in pitch perfect scams that lead to the divulging of personal credentials, downloading malware or allowing remote access. This can give the fraudster control of accounts, personal data and payments that may well come via a fully authenticated login session or customer-initiated action.

The weekly headlines of fresh data breaches and further identity leakage, with millions, if not billions, of identity data points available in the wild, make such attacks all the more successful. How do businesses walk the unsteady path of ensuring effective fraud control, customer data privacy and a low-friction online environment, particularly when faced with evolving regulatory reform and robust fines for non-compliance?

The most effective mitigation to this tidal wave of attack vectors lies in a layered defense solution; one that combines the full gamut of digital and physical identity verification and authentication strategies so that businesses can gain a single view of their end consumer across their entire journey, both on and offline. This relies on being able to build and access a comprehensive, reliable and real-time view of identity, capturing the unique specificities of customer behavior on a per-user basis, bolstered by strong authentication strategies that leverage information the user knows, possesses or inherently is.

LexisNexis®
RISK SOLUTIONS

Report Overview

The LexisNexis® Risk Solutions Cybercrime Report is based on cybercrime attacks detected by the LexisNexis® Digital Identity Network® from January – June 2019, during 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 behavioural analytics.
- The Digital Identity Network and its real-time policy engine provide unique insight into users' digital identities, even as they move between 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 discussed are from "high-risk" transactions scored by LexisNexis® Risk Solutions customers.
- LexisNexis® Risk Solutions analyzed 16.4 billion transactions January-June 2019, with 62% originating from a mobile device.

LexisNexis®
RISK SOLUTIONS

January-June 2019 in Numbers

16.4 Billion
Transactions Processed

277 Million
Human-initiated Attacks

13% Growth in 6 months

62%
Mobile Transactions

Including

111 Million
Mobile Attacks

9% Growth in 6 months

United States
Biggest Attacker by Volume

2.1%
Attack Rate

The LexisNexis® Risk Solutions Identity Abuse Index

The LexisNexis® Identity Abuse Index shows the percentage of attacks per day, across the entire Digital Identity Network, providing a good indicator of how attack patterns have changed and evolved over the past two years, and the impact large data breaches have on global cybercrime.

The Digital Identity Network recorded a much more benign environment in the first half of 2019 in comparison to the two preceding years, with 2017 and 2018 dominated by high volume bot attacks originating from diverse and emerging economies. The smaller peaks in 2018 can be attributed to attacks originating from new geographies, indicating the wide dispersal of breached identity data to all corners of the globe.

However, although the first six months of 2019 were less volatile than previous years, the Digital Identity Network did record a significant spike in June. Recorded as the highest peak in attacks over the last two years, a virtual gift card provider was targeted with a series of bot attacks that were testing different email addresses from just one IP address. Interestingly, the attack originated in the U.S., as shown in the IP based location, but the browser language was set to Russian.

The Digital Identity Network also recorded two smaller peaks in attacks in the first six months of 2019; in January, a global e-commerce merchant was the key target for a series of bot attacks coming from the U.S., Chile, Switzerland and Canada. These bots were attempting fraudulent new account creations from desktop devices, using stolen identity credentials. In February, fraudsters used device spoofing and IP spoofing to target a multinational bank, with the attacks originating from the U.S.

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

The most significant spikes in attacks often coincide with big data breaches in the news.

Identity Abuse Index over the last 2 years

Bots Evolve to Target New Account Creations in E-commerce and Media

The key difference in bot attacks during the first six months of 2019 has been the growth in bots targeting new account creation transactions.

Although account logins remain the primary attack target by volume, new account creations is the only use case that recorded a growth in attacks during the period.

Bot attacks from India and South East Asia have seen considerable growth over the last year, suggesting growth economies are becoming an integral part of the global cybercrime economy.

Fraudsters are often using these new account creation attempts to test, validate and build online identities for financial gain. However, there are a number of other scenarios at play:

The media industry is seeing a number of bonus abuse attempts; fraudsters are using bots to sign up for mass new media accounts to take advantage of free trials / streaming bonuses that can be sold on for a profit.

In e-commerce these new account creation bots are seen at online marketplaces, virtual gift card companies and ridesharing sites.

Online marketplaces give fraudsters the opportunity to access seller credentials, make fraudulent bids or phony listings.

Virtual gift cards offer a way to quickly monetize stolen credit cards; they can be spent immediately or sold on.

At ridesharing sites, fraudsters are creating fake rider/driver accounts to monetize stolen credit cards and target the increased commission drivers receive through completing a set number of journeys. Both accounts use GPS spoofing apps to make the journeys appear legitimate, while the scammer pockets money from the stolen credit card and the ridesharing company.

INDUSTRY TREND: E-commerce

E-commerce New Account Creations
Bot Attack Growth

171% YOY

305% in 6 months

INDUSTRY TREND: Media

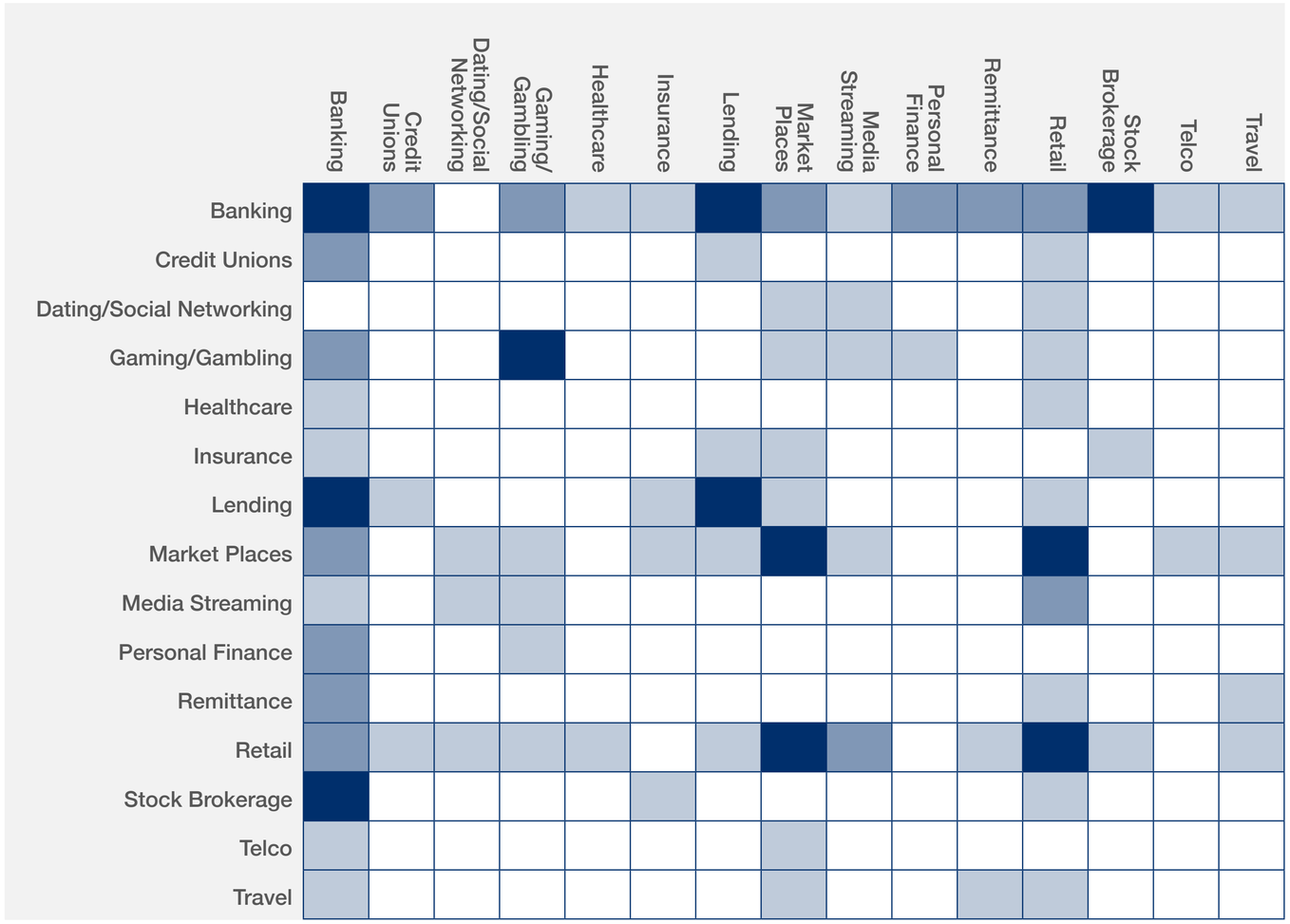
Media New Account Creations
Bot Attack Growth

123% YOY

65% in 6 months

The Growing Threat of Networked Cybercrime

Heat Map Showing Level of Shared Fraud Across Organizations



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

This footprint of networked cybercrime emerges when digital identities are associated with confirmed fraud attempts across more than one organization.

The strongest correlation of fraud (as shown by the darkest colors in the heat map opposite) continues to be across organizations within the same industry, particularly banking, lending and stock brokerage.

Banking in particular has a high level of shared fraud with nearly all other industries. Bank accounts are an integral part of financial crime, enabling and facilitating the laundering of money and proceeds of crime.

While this heat map shows the holistic view of networked fraud, the story on the following page shows how this phenomenon plays out across 6 different organizations and three different industries.

LexisNexis® RISK SOLUTIONS

Tracking the Path of a Fraudster Across Different Industries and Global Organizations

Fraudster:

- One fraudster operating from the UK
- Using one device, but attempting to bypass device fingerprinting

Target:

- A series of global organizations including multiple financial services organizations, a media streaming company and a credit reporting agency

Method:

- The fraudster carried out a large number of transactions across 6 different organizations, attempting fraudulent new account creations, bonus abuse and money laundering
- The fraudster even created an account with a credit reporting agency, presumably aiming to augment stolen identity data to make fraudulent account creations more successful
- While some of these these transactions were flagged as high-risk or blocked as fraud, some were processed

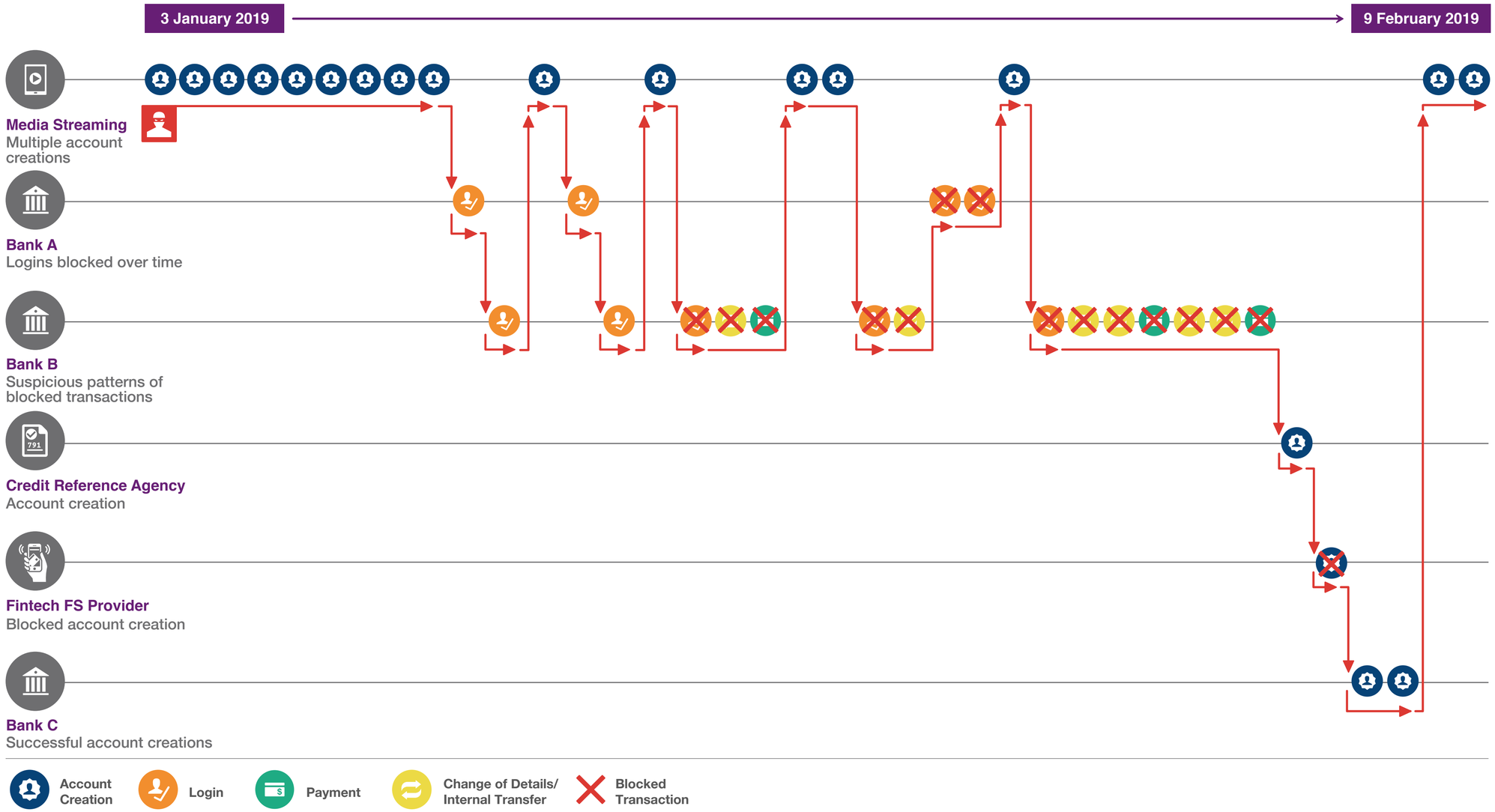
The Digital Identity Network Benefits:

- LexisNexis® Risk Solutions enables organizations to tag and share tokenized intelligence related to high-risk behavior in near real time, benefitting from a shared view of risk
- Persistent device recognition provides a common identifier across the Digital Identity Network
- A unified digital identity enables fraudsters to be tracked across devices, locations and credentials
- LexisNexis® Risk Solutions customers manage their own risks, tailoring rules to their own risk appetite
- Leveraging customer performance and feedback helps to inform better and more dynamic decisions

Consortium Benefits:

- Consortium allows LexisNexis® Risk Solutions customers to share information to collectively fight fraud
- Consortium creates an industry-focused and/or peer-based layer that complements an organization's local intelligence and the global shared intelligence harnessed through the Digital Identity Network
- This enables businesses with common goals, challenges or fraud risks to share their negative and positive data attributes in near real time, across an agreed set of Consortium members and contributors

Tracking the Path of a Fraudster Across Different Industries and Global Organizations



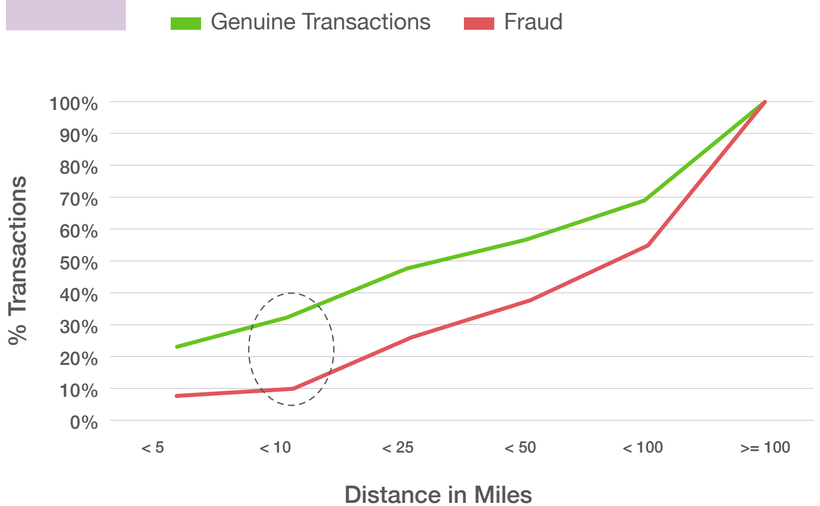
LexisNexis® RISK SOLUTIONS

Location Intelligence is Key Risk Indicator for Financial Services Transactions

The physical location of a customer making a financial services payment transaction can be a key indicator of trust or risk, as evidenced below where location attributes are proven to be indicative of fraudulent behavior.

As well as capturing the IP address of a transacting user, LexisNexis® Risk Solutions intelligence can also detect the use of proxies, VPNs and the TOR browser. In the case of proxies and VPNs, LexisNexis® Risk Solutions allows organizations to risk assess the IP address, geo-location and other attributes of each transaction.

Distance Between IP Based Location and Home Address of Customer



A short distance between IP based location and home address of customer is more than three times as likely to be a good payment.

Distance Between Customer and Beneficiary Account

A short distance between customer and beneficiary account is more than twice as likely to be a good payment. Conversely, a larger distance is more than twice as likely to be fraud.

Monitoring Events from Sanctioned Countries

Leveraging the power of the Digital Identity Network, LexisNexis® Risk Solutions is now enabling organizations to recognize transactions from sanctioned countries, regardless of which business saw that behaviour. By combining these data points with digital identity intelligence, LexisNexis® Risk Solutions is seeking to help its customers better manage compliance requirements, and respond to potential threats arising from attempts to move money illicitly while potentially masking true location. When aligned with watchlist screening capabilities, this presents a more holistic assessment of fraud and financial crime risks.

Analyzing consumer behaviors and transaction patterns from sanctioned countries reveals a number of attempts to purposefully cloak true locations through the use of proxies.

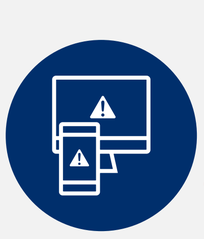
However, transactions that originate in a sanctioned country are not necessarily made by bad actors in the financial system, but may simply come from people travelling for work or leisure, or visiting families abroad.

LexisNexis® Risk Solutions can help organizations layer intelligence relating to locations with other high-risk markers such as use of proxies in non-sanctioned countries.

This intelligence can add further context to the wider network of associated transactions and help prevent financial crime related activities.

Once identified, bad actors and high-risk transactions can be screened against LexisNexis® Risk Solutions global watchlists to help with an organization's Enhanced Due Diligence and required Risk-Based Approach.

Monitoring Events from Sanctioned Countries During 1 Month



460K
devices seen in sanctioned countries

44K A subset of these devices were also seen in non-sanctioned countries (mostly through financial services organizations)

13K A significant number of devices were using a proxy in a non-sanctioned country, indicating potentially illicit money movements / suspicious behaviors

64 Some of these devices have subsequently been proven to be associated with confirmed fraud. However, the true value may be significantly higher depending on outcomes of further financial crime investigations / Suspicious Activity Reports

Consumers Benefit From the Lower Attack Rate on Mobile Transactions, but Fraudsters Eye Their New Target

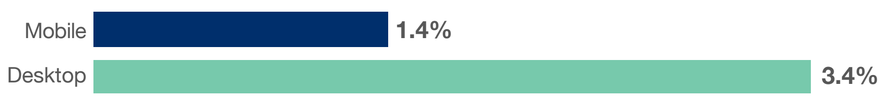
The balance of mobile to desktop transactions continues to tip further in favor of mobile, with a 12% growth in the proportion of mobile transactions in the last year alone. New account creations see the highest penetration of transactions coming from a mobile device, at 66%.

Across all industries and use cases, mobile transactions are attacked less than half as much as desktop transactions, largely due to the inherent security features of mobile devices.

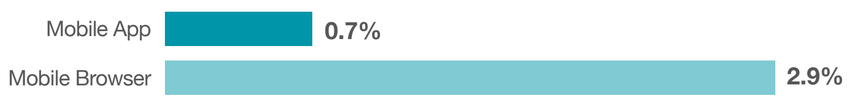
Mobile app transactions are also 4 times safer than mobile browser ones, indicating that fraudsters see mobile browser transactions as an easier target. Mobile apps tend to involve a pre-registration, or additional layers of authentication, whereas mobile browser transactions can be isolated events. In addition, many organizations prevent users registering for apps if their phone is jailbroken or rooted. Authentication can also leverage the inbuilt biometric features of the device for added security.

There are, however, pockets of growth in mobile attack rates, specifically across payments transactions (all industries), and new account creations in financial services and media. This indicates that fraudsters are eyeing a potentially lucrative new target and following the volume shift to mobile.

Attack Rate: Mobile vs. Desktop



Attack Rate: Mobile App vs. Mobile Browser



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 real time depending on individual customer use cases.

Mobile Helps Drive Financial Inclusion in Growth Economies, but at a Higher Cost

India and South America have both experienced strong growth in mobile penetration rates year-on-year, at 33% and 30% respectively, compared to a global average of 14%.

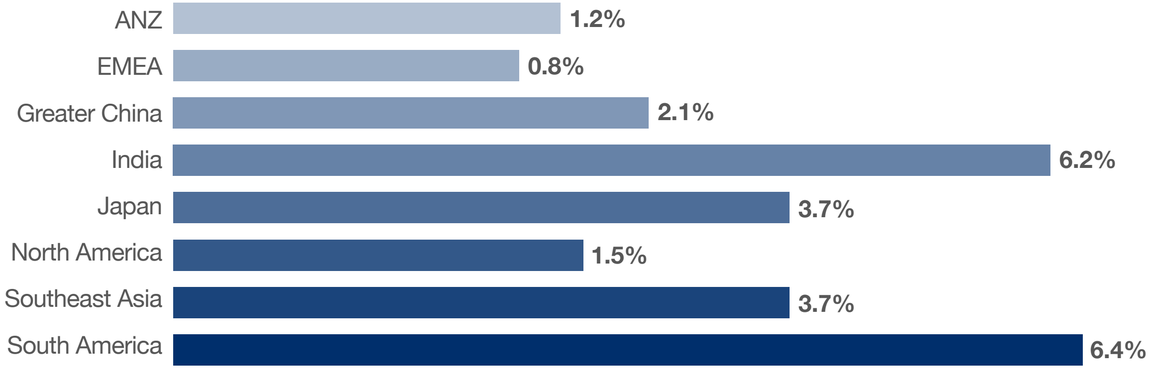
Smartphone use in these regions can offer a gateway to digital transacting, providing consumers with access to online goods and services, as well as social media platforms.

Mobile also continues to be a key enabler for financial inclusion of the unbanked and underbanked consumer population, who can use mobile devices to carry out money transfers, sign up for microloans, and access online banking services when physical branch facilities are not available.

However, the attack rate in these regions is also higher, indicating that fraudsters are seeing opportunity in targeting emerging products and services, as well as the consumers who are accessing them.

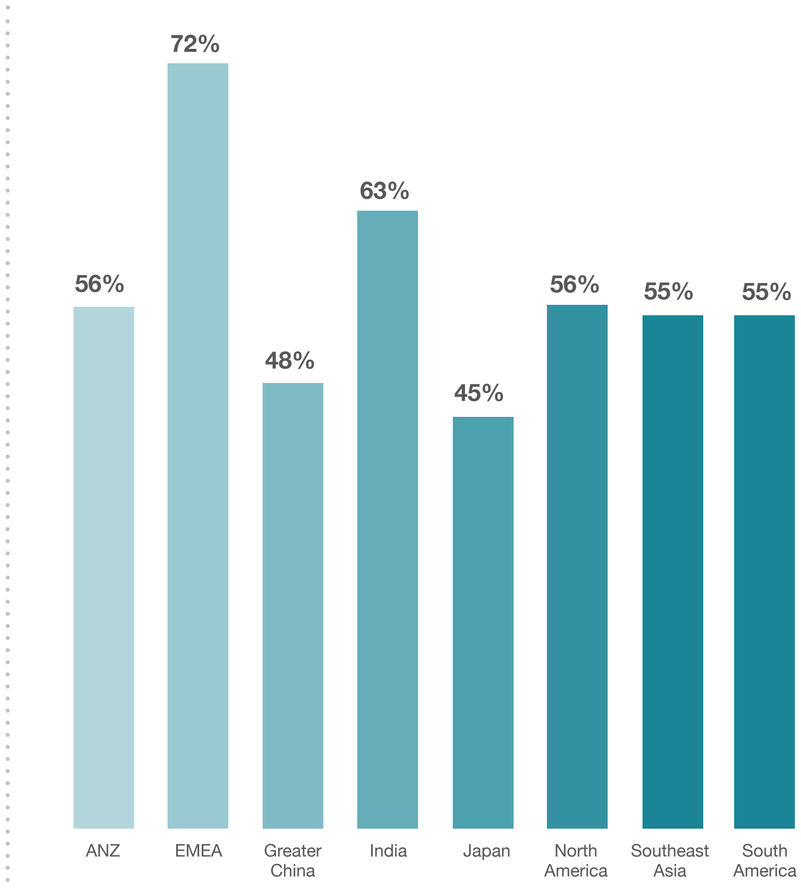
South America in particular, has seen a growth in the mobile attack rate on all financial services transactions, as fraudsters target consumers new to mobile banking with evolving attack vectors.

Attack Rate per Region



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 real time depending on individual customer use cases.

Mobile Penetration by Region



Fraudsters Target Mobile App Registration as Key Vulnerability in the Customer Journey

On mobile devices, fraudsters are seeing new account creations, or app registrations, as key opportunities to mimic good customers, or pass security checks, sometimes intercepting one-time passcodes to fraudulently register a mobile app.

In financial services, this can provide fraudsters with direct access to a customer's bank account; an existing account holder may simply be adding mobile banking as an additional channel to manage their account.

Globally, these attacks on mobile apps are skewed towards media organizations, particularly targeting social media and gaming / gambling organizations. There are a number of potential scenarios at play, including:

- Mobile account creation bots targeting social media apps to test, validate or build synthetic identities. The Digital Identity Network saw hundreds of thousands of bot events from Russia, Indonesia, Brazil, Thailand, India, Ukraine and Bangladesh, suggesting stolen / synthetic identity farms may be supporting emerging and growth economies.
- In gaming and gambling, fraudsters are likely registering for new player bonuses that might be sold on for profit.

GLOBAL TREND

Mobile App Registration Attack Rate Growth

4% YOY

144% in 6 months

INDUSTRY TREND: Media

Mobile App Registration
Attack Rate Growth

324% YOY

148% in 6 months

REGIONAL TREND

South America:
Finance Mobile App Registrations at risk

All regions see growth in
Media Mobile App Registration attacks

Mobile Browser Vulnerability for Global Financial Services Transactions

REGIONAL TREND

Seen in North America, South America, China and ANZ

INDUSTRY TREND: Financial Services
Mobile Browser Attack Rate Growth

New Account Creations		Payments
45%	YOY	38%
10%	In 6 Months	9%

REGIONAL TREND

Seen in EMEA and South America

Online banking continues to shift towards the mobile channel in a number of regions; EMEA has the highest penetration of mobile transactions for financial services at 81%, while South America is seeing the biggest growth in mobile penetration year-on-year at 60%.

While full service mobile banking apps drive the majority of this volume shift, there is also a sizeable proportion of mobile transactions made on mobile browsers.

It is these mobile browser transactions that are being targeted by fraudsters, presumably because they are seen as an easier target in comparison to the tighter security framework associated with mobile apps.

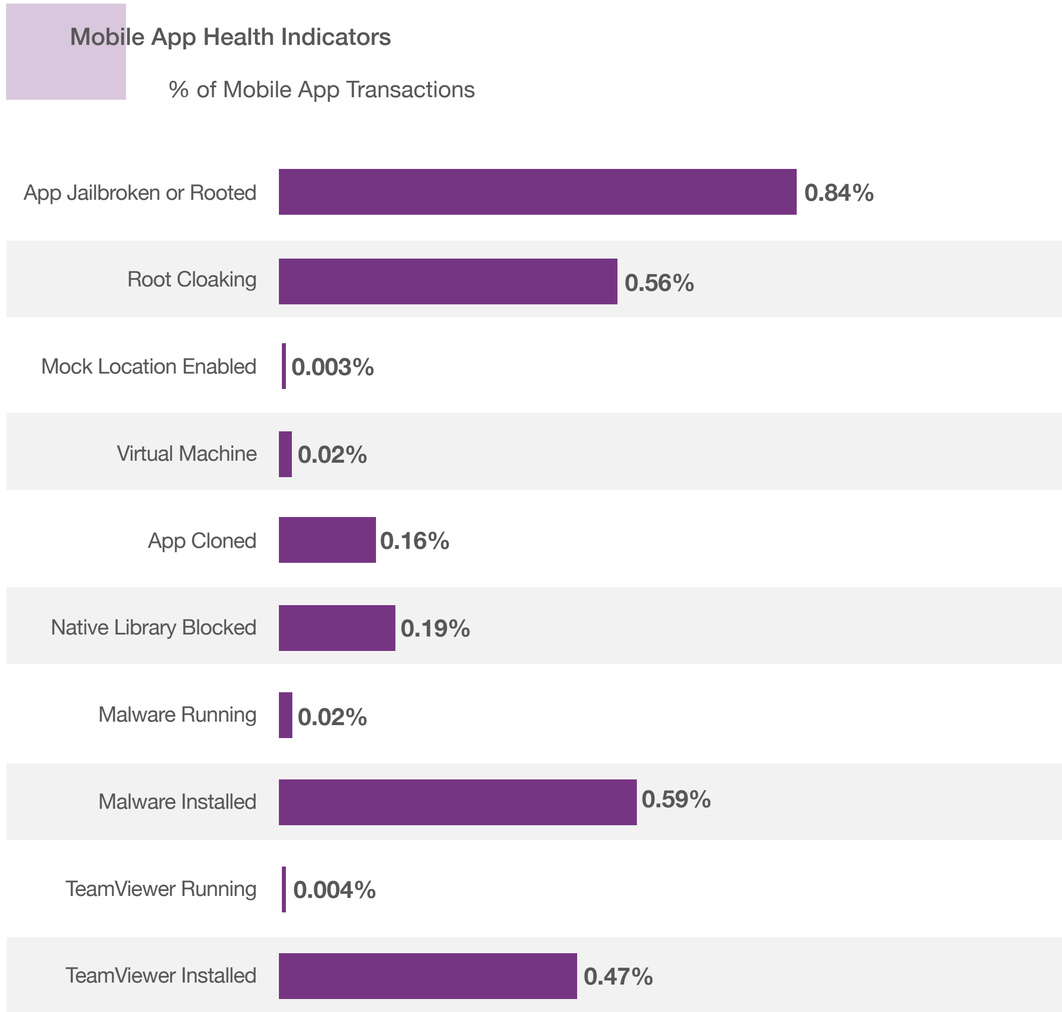
There has been a growth in mobile browser attacks across both new account creations and payments transactions during the first half of 2019. There are regional nuances to these growth rates; the new account creation attack growth is seen largely in the Americas, China and ANZ, while the payments attack growth is seen predominantly in EMEA and South America.

Layers of Defense for Mobile Apps

Being able to detect potential risks on a mobile app can help businesses protect themselves and their customers from malicious threats. The LexisNexis® Software Development Kit (SDK) can detect a number of potentially high-risk scenarios in real time, which can often be indicators of current or future fraud.

For example:

- Identifies devices that have been jailbroken or rooted
- Identifies devices on which fraudsters have attempted to mask the signs of a rooted device
- Detection of apps using a mock location for their GPS data
- Detects instances where a genuine app has been cloned, either totally, or using cloning software, on the same device
- Evaluates all installed applications on Android devices and verifies them against a signature database of over 15 million mobile apps
- Detects presence of malware, either installed and/or running
- Detects the presence of remote access software, either installed and/or running



LexisNexis® RISK SOLUTIONS

Global Transaction Patterns and Attack Rates

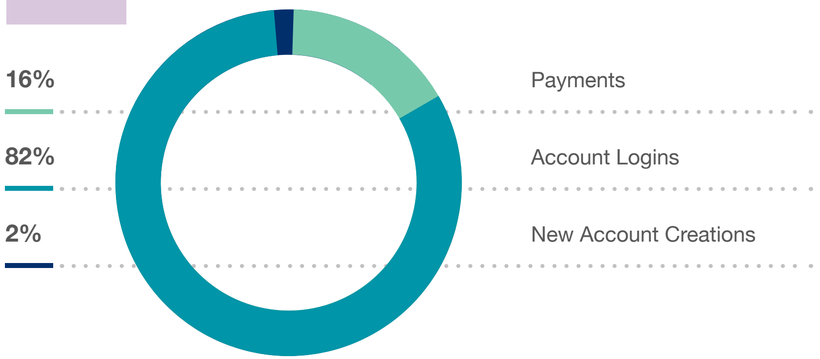
LexisNexis® Risk Solutions helps organizations assess trust and risk across the entire customer journey, from new account creations and logins, to password resets/ change of details and payments. Providing universal fraud and authentication decisioning across all use cases, and across all customer touchpoints, LexisNexis® Risk Solutions transactions span the full spectrum of global industries, from e-commerce, financial services and media, to gaming and gambling, telco and insurance.

Global transaction patterns and attack rates have remained largely consistent over the past few years. Login transactions are attacked at the lowest rate, in part because the high volume of transactions helps organizations build trust over time with consistent repeat behavior. Conversely, new account creations continue to have the highest attack rate of all the use cases analyzed by the Digital Identity Network. Around 1 in 6 new account creations is identified as high-risk, with significant acceleration in the last six months and increasing 24% year-on-year. This growth is indicative of the lucrative opportunities new accounts can afford cybercriminals; bad actors use stolen identity credentials harvested from data breaches to open fraudulent accounts and perpetrate further criminal activity, such as applying for loans or monetizing stolen credit cards.

Looking to regional hotspots, 1 in 4 new account creation transactions is identified as an attack in China, the highest of all regions analyzed. Interestingly, although Greater China rejects a higher percentage of new account creation transactions than any other region, North America has seen the biggest year-on-year growth in rejected new account creation transactions, at 152%.

Payments transactions in India are rejected at a rate of 1 in 6, the highest of all regions. This may also be indicative of the wider payments landscape in India; there has been a recent surge in new entrants to the mobile payments industry, with new mobile payments providers offering risk and reward for both consumers and fraudsters.

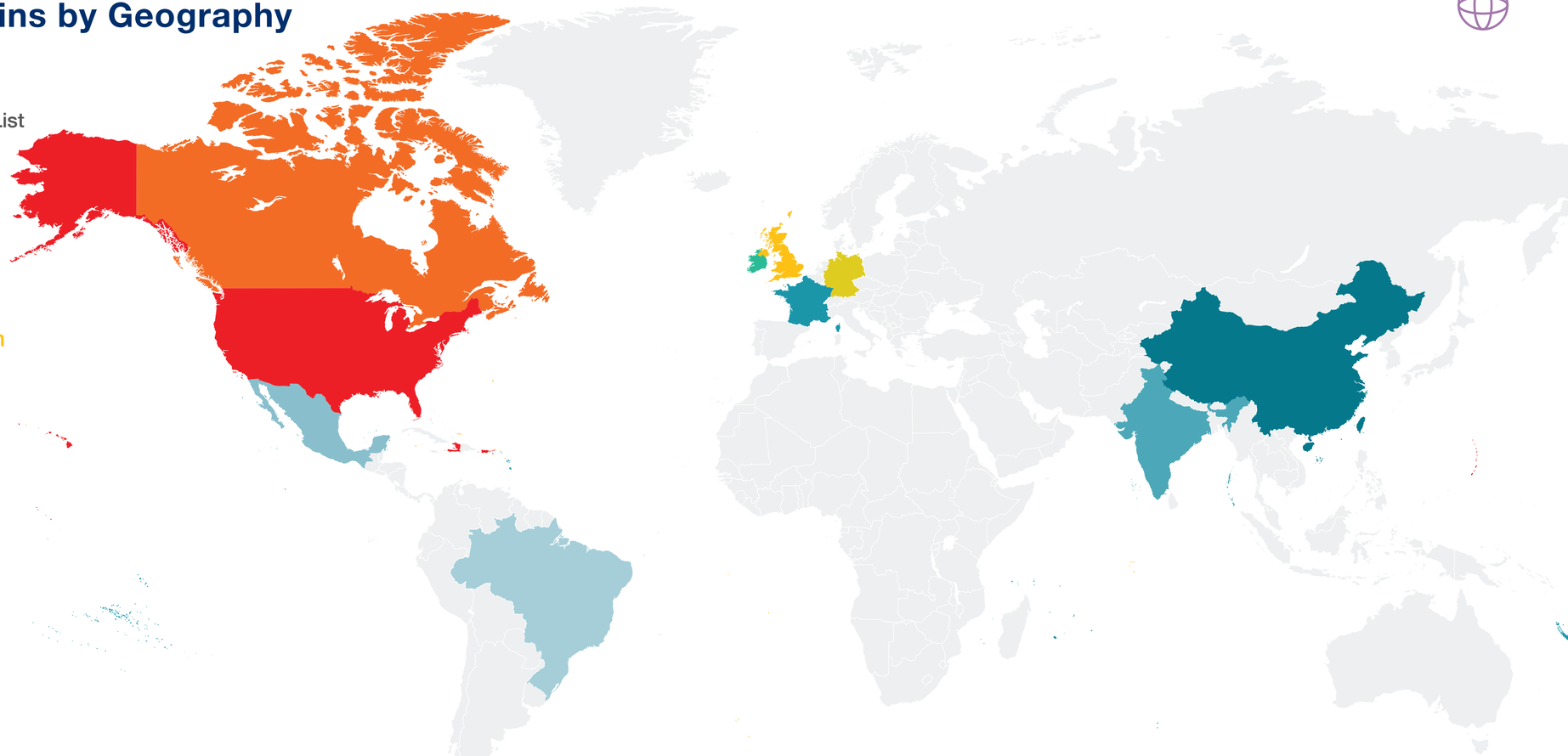
Volume per Transaction Type



Attack Rate per Transaction Type

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 real time depending on individual customer use cases.

Attack Origins by Geography



Top 10 Attackers List

#1 United States

#2 Canada

#3 United Kingdom

#4 Germany

#5 Ireland

#6 Brazil

#7 Mexico

#8 India

#9 France

#10 China

Cybercrime is now an established industry in its own right and, like any growing enterprise, continues to expand with highly organized, customizable services and regional outposts in emerging economies.

The largest attack volumes have consistently originated from the economic powerhouses of the U.S., UK and other large European nations.

However, as breached identity data becomes more widespread, fueling the growth of cybercrime across borders and continents, a noticeable shift towards attacks originating from growth economies has emerged.

Mexico is a notable emerging economy making its debut on the top ten attackers list, having climbed six places in the last 12 months. A possible explanation for Mexico's rapid rise to the top 10 rankings is the current heightened risk environment in the LATAM region; the incredibly diverse region is in the midst of immense digital growth and has emerged as a hotbed of new account creation fraud. This may also explain Brazil's repeated top 10 ranking.

The first half of 2019 also recorded a growth in attacks from Bangladesh, Malaysia, Pakistan and Colombia, illustrating the global nature of cybercrime.

Top Attack Originators and Attack Destinations

In the first six months of 2019, fraudsters from the top 5 attacking nations have targeted the biggest digital economies in the world; the United Kingdom, United States and Canada consistently appear as top attack destinations.

Typified by a large proportion of the population transacting online, in addition to a high mobile penetration, fraudsters see these countries as target-rich environments. High-volume digital traffic can be used by fraudsters as perfect camouflage for nefarious, fraudulent transactions.

Interestingly, there are fewer emerging and growth economies in the list of destinations that fraudsters are targeting, which sits in contrast to the 2018 rankings which included Brazil, Colombia and Bulgaria. However, these economies are still being targeted, just at a lower volume.

Argentina is, however, one emerging economy which did rank as a top destination, attracting attacks from the U.S. The majority of attacks targeting Argentina were directed at an e-commerce merchant, with a sustained attack targeting logins and payments using different email accounts, but originating from the same device.

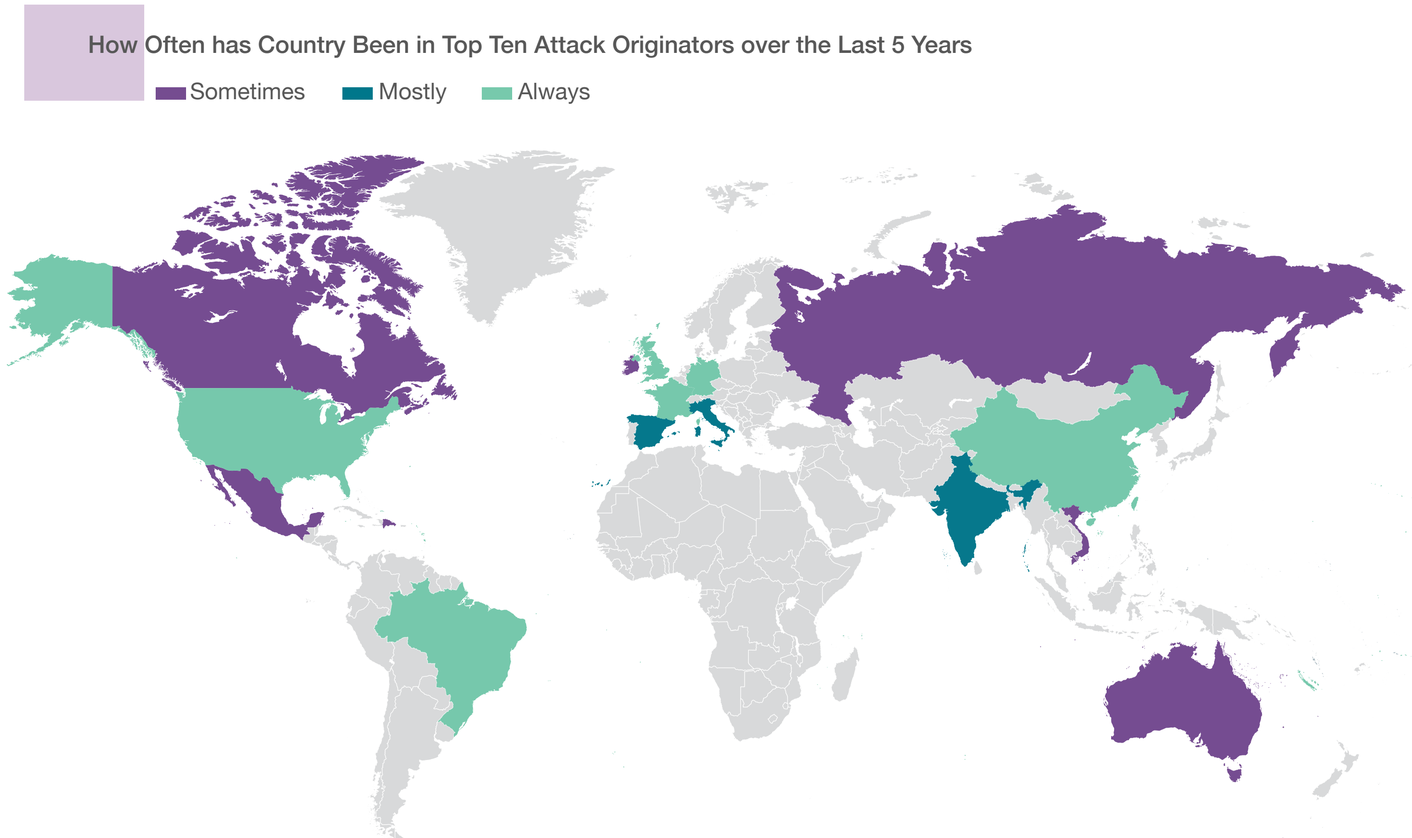
Top 10 Attack Originators 2015-2019

Analysis of the top 10 attack originators over the last five years gives a compelling insight into how global cybercrime has grown and disseminated to almost all corners of the world.

The list of top attacking nations reflects how diverse, widespread and truly global cybercrime is today. No longer just the preserve of the more digitally advanced, economic powerhouses, cybercrime has spread across continents with established regional outposts in growth and emerging geographies.

As the analysis shows, the top 10 attack originators are now spread across 5 continents, with the bigger economies of the UK, China and U.S. joined by growth economies including India, Mexico, and Vietnam.

Interestingly, Brazil matches the UK, U.S., Germany and France with the number of times it has ranked as a top attacking nation. Brazil's consistent inclusion as a top attacking nation is indicative of the country's strong cybercrime footprint and its increasingly prominent role on the cybercrime world stage.



Region Spotlight: North America Sees High Rate of Fraudulent New Account Creations

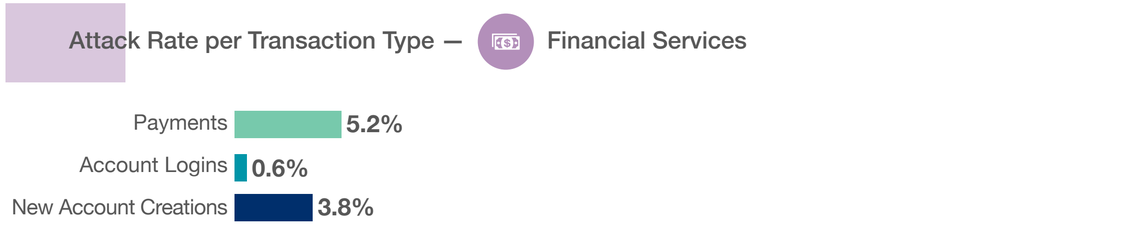
Data breaches continue to make headline news in North America, with estimates suggesting 60 million Americans have been affected by identity theft.[1] In some cases, identity data may have been stolen several times over, with fraudsters continually validating and building stolen and synthetic identities to improve the success of attacks.

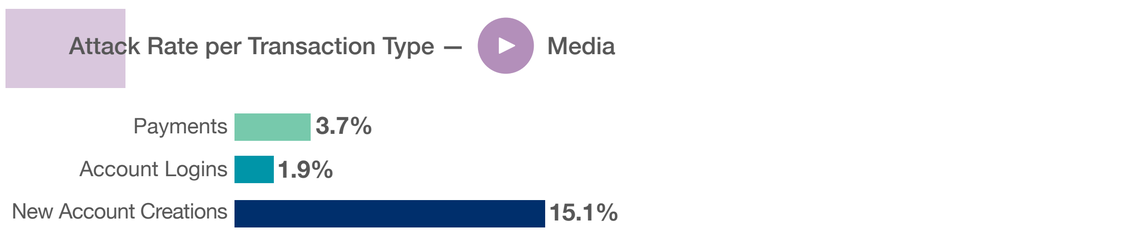
The impact of these breaches is highlighted in the e-commerce new account creation attack rate. Globally the attack rate is 30.4%, but in North America the attack rate is almost 40%, with this risk growing faster than the global rate year-on-year. Desktop transactions are by far the biggest target for these attacks. This was heavily influenced by a large and sustained attack on a virtual gift card company during the first half of 2019.

A large proportion of these new account creations attacks are carried out by automated bots trying to validate, augment or build out identities, or attempting to benefit from new account bonuses or discounts. The bot attack rate on new account creations in North America is also growing at a faster rate year-on-year in comparison to globally.

The e-commerce payments attack rate from North America is also slightly higher than the global figure, and growing at a rate of 52% year-on-year compared to 12% globally. This highlights the fact that EMV migration continues to push payment fraud online.

[1]Harris Poll, 2018, www.theharrispoll.com





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 real time depending on individual customer use cases.

Region Spotlight: U.S. Sees Higher Attack Rate Compared to Similar Economies Globally

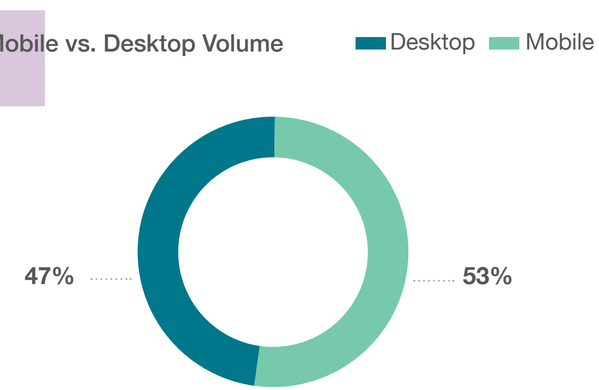
Just over half of all transactions from the U.S. come from a mobile device, a slightly lower percentage than some of its nearest economic neighbors such as Canada and the UK.

Some commentators suggest that mobile banking adoption has slightly plateaued in the U.S. This may be contributing to a downtick in mobile transaction penetration in comparison to the UK and Canada, which both see very high mobile banking login penetration at 86% and 71%, respectively. The U.S., in comparison, sees a penetration rate of 53% for mobile banking logins.

In addition, the U.S. sees a higher attack rate overall than either Canada or the UK, particularly on desktop transactions, highlighting that a higher mobile penetration rate seems to correspond to a lower overall attack rate.

In terms of attack vectors, identity spoofing is the most prevalent attack vector in the U.S., followed closely by device spoofing.

Mobile vs. Desktop Volume



Attack Rate per Transaction Type

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 real time depending on individual customer use cases.

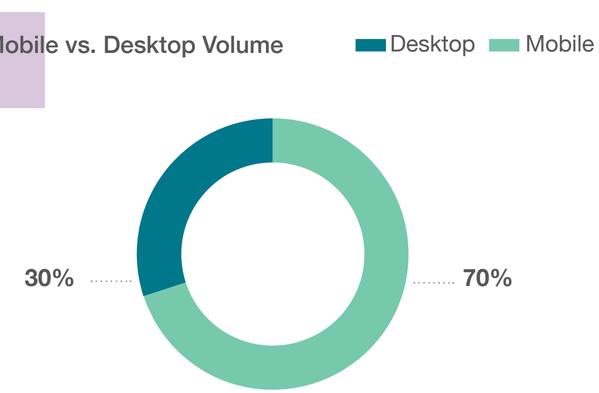
Region Spotlight: High Mobile Penetration in Canada Helps Drive Lower Overall Attack Rates

Canada is the second largest originator of financial services attacks in the Digital Identity Network, second only to the U.S. However, for Canada this strong attack position seems to go hand-in-hand with a slightly more advanced online banking industry, with almost three quarters of Canadians using digital channels to do most of their banking transactions.[1]

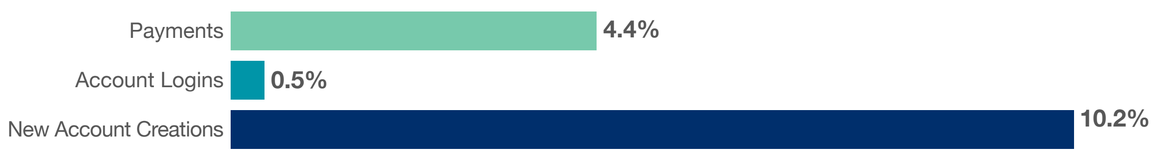
Although the higher mobile penetration rate seems to correspond with lower attack rates overall, the attack rate on mobile browser transactions is comparatively high, and higher than the U.S. figure.

In line with trends in the U.S., identity spoofing is the most prevalent attack vector, followed by device spoofing. However, the percentage of attacks that are recognized as both identity spoofing and device spoofing is lower in Canada in comparison with the U.S.

Mobile vs. Desktop Volume



Attack Rate per Transaction Type



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 real time depending on individual customer use cases.

[1]Canadian Bankers Association, 2019, https://cba.ca/technology-and-banking

E-commerce Emerges as Key Target for New Account Creations Attacks as Fraudsters Pivot on Different Industry

As merchants vie for customers in an increasingly crowded marketplace, promotional discounts, offers and free trials are designed to attract market share. Cybercriminals, however, see opportunity in these promotions, for example illegally signing up for, and then selling on free trial accounts on a mass scale. In addition to taking advantage of discounts and other promotions, new accounts can also be used by fraudsters to make payments with stolen credit cards.

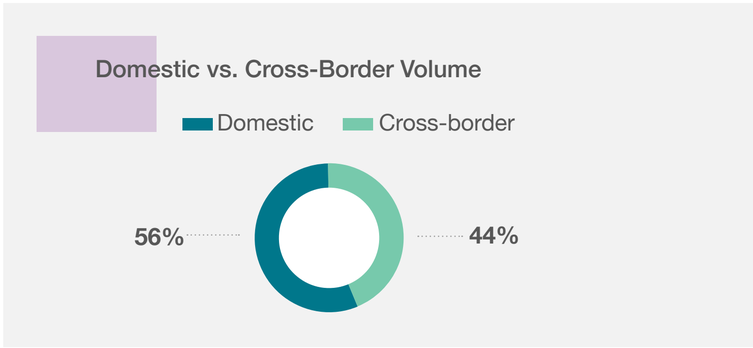
In the first six months of 2019, an extremely high percentage of attacks were recorded on new account creations, illustrating how e-commerce continues to be a prime target for monetizing stolen identity credentials gleaned from data breaches.

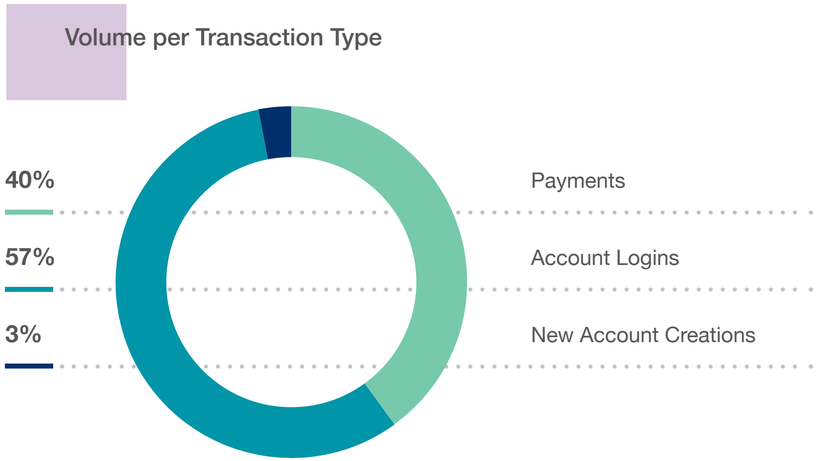
The attack on a virtual gift card provider in June contributed to the high percentage of attacks on new account creations, although the attack rate is also indicative of the heightened risk the industry faces from fraudulent new accounts.

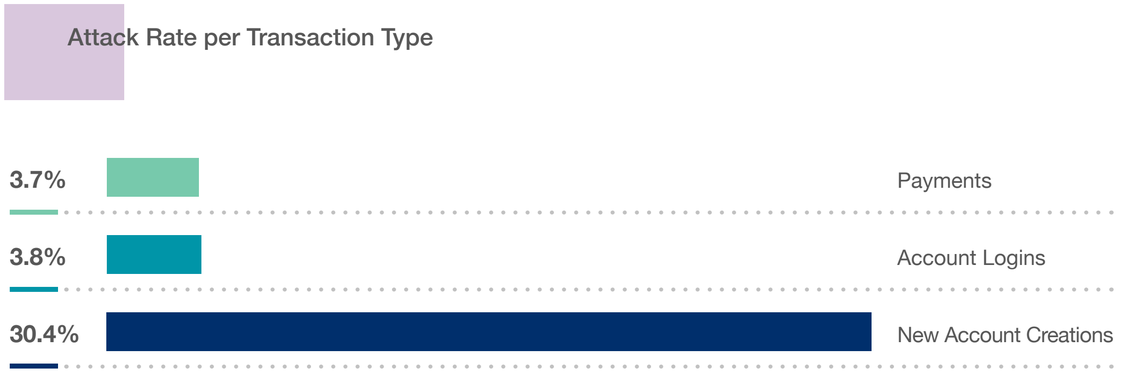
While mobile plays a prominent role in e-commerce transactions, they are still more desktop-based than other industries. 69% of e-commerce login transactions originate from a desktop device, suggesting that consumers still prefer a bigger screen when browsing online marketplaces, even if mobile is the preferred device at payments.

The Digital Identity Network also recorded a 13% growth in the penetration of mobile payments in e-commerce year-on-year. This has impacted the cybercrime landscape, however, with mobile app payments seeing a significant growth in attack rates.

E-commerce merchants enjoy a truly global customer base, with consumers searching for the best deals and services regardless of location. Merchants are increasingly targeting consumers outside their country of origin: 44% of all e-commerce transactions are now cross-border. This presents merchants with additional challenges around identity verification, authentication and fraud control, demanding a global view of digital identity and fraud risk.







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 real time depending on individual customer use cases.

LexisNexis® RISK SOLUTIONS

Spotlight: Malaysian Bot Attack Targets Major U.S. Retailer with Sustained Account Takeover Attempts

Fraudster:

- Bot Attacker from Malaysia, with some attacks originating from Russia and the U.S.

Target:

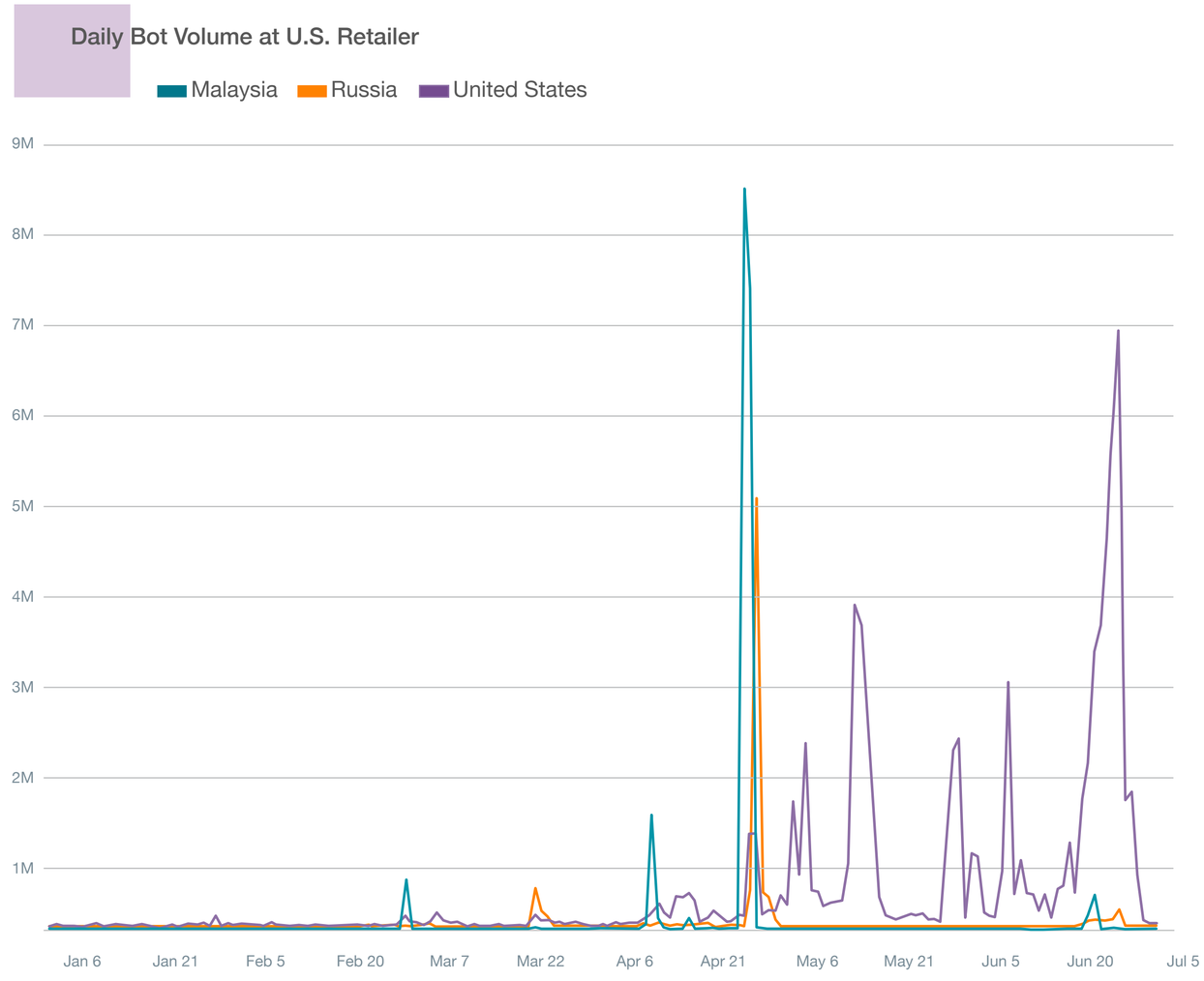
- Major U.S. Online Retailer

Method:

- High velocity bot attacks targeting account logins

Attack:

- 130 million logins attempted, using 33 million email addresses in the last six months.
- During one attack in May, daily traffic increased from 400,000 login transactions, to 9 million.
- The bot operator used one email address originating from multiple IP addresses in an attempt to avoid detection.



High Mobile Penetration in Financial Services See Fraudsters Target Mobile Browser Transactions

The impact of the evolving digital economy on financial services has been transformative, with digital technologies, regulatory reform and fintech providers constantly challenging the way that consumers interact with their providers, and the services that financial institutions offer. At the same time, organizations are being forced to adapt to often competing demands of security, customer privacy, competition and low friction access to online services.

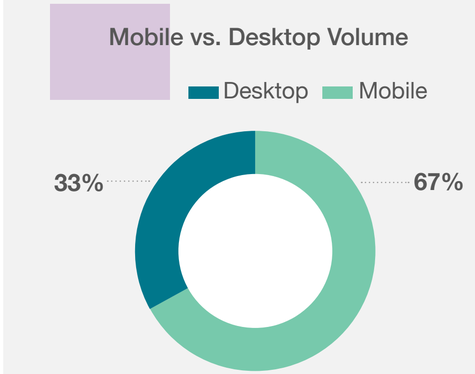
A key driver behind the transformation in financial services is mobile technology, with consumers showing varying degrees of preference for full service banking apps and online transacting. The Digital Identity Network recorded 67% of financial services transactions originating from a mobile device in the first half of the year; a growth of 6% from the previous half year and a 34% increase year-on-year.

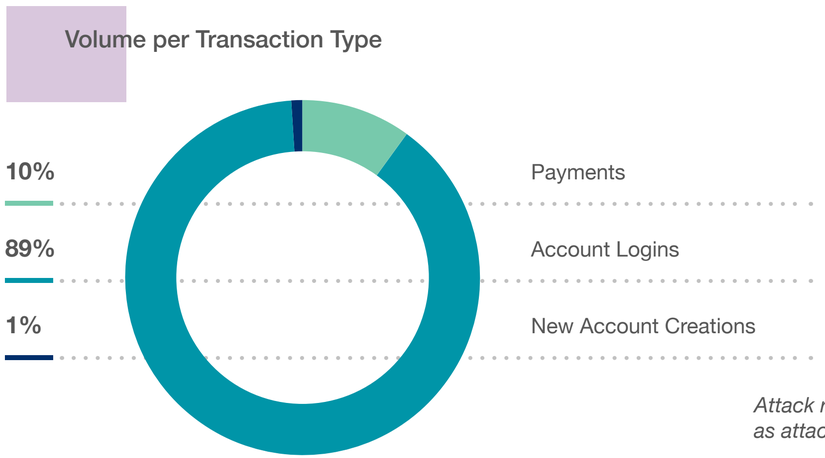
This volume shift to mobile, however, has not gone unnoticed, with fraudsters evolving attacks in order to tap the increasingly lucrative mobile channel. Fraudster's have identified that mobile apps have a key vulnerability at the point of registration, illustrated by the 38% year-on-year growth in attacks on new account creations in the mobile channel.

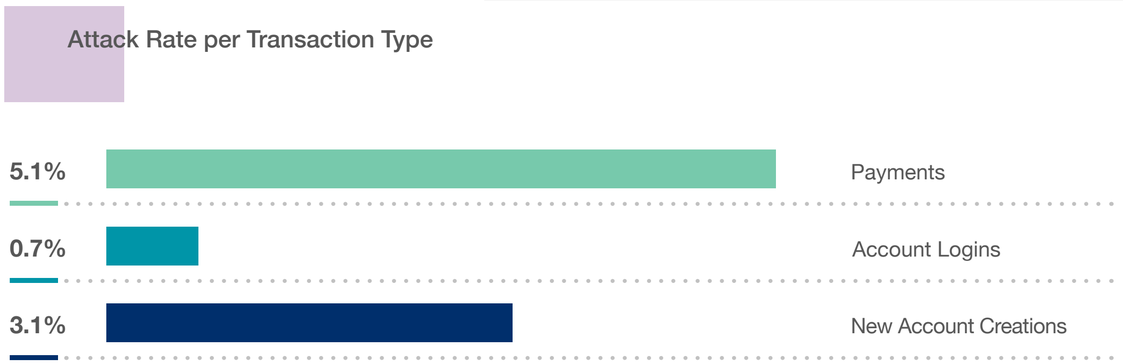
There was further noticeable growth in transactions made via mobile browser; a 45% year-on-year growth in attack rate was recorded on new account creations made through mobile browsers. Payments, interestingly, also saw a 38% year-on-year growth in attack rate on transactions via mobile browser.

Both new account creations and payments have seen growth in identity spoofing; 58% year-on-year for new account creations, and 24% year-on-year for payments.

Fraudsters are likely targeting these transactions with sophisticated impersonation attempts, in efforts to establish a fraudulent account and potentially launder money through the financial system.







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 real time depending on individual customer use cases.

Spotlight: Helping a Payment Processor Detect Fraudulent or Unauthorized Merchants by Analyzing Referrer Domain Attributes

Target:

- Payment processor, who could unwittingly be processing a fraudulent or illegal payment

Fraudster:

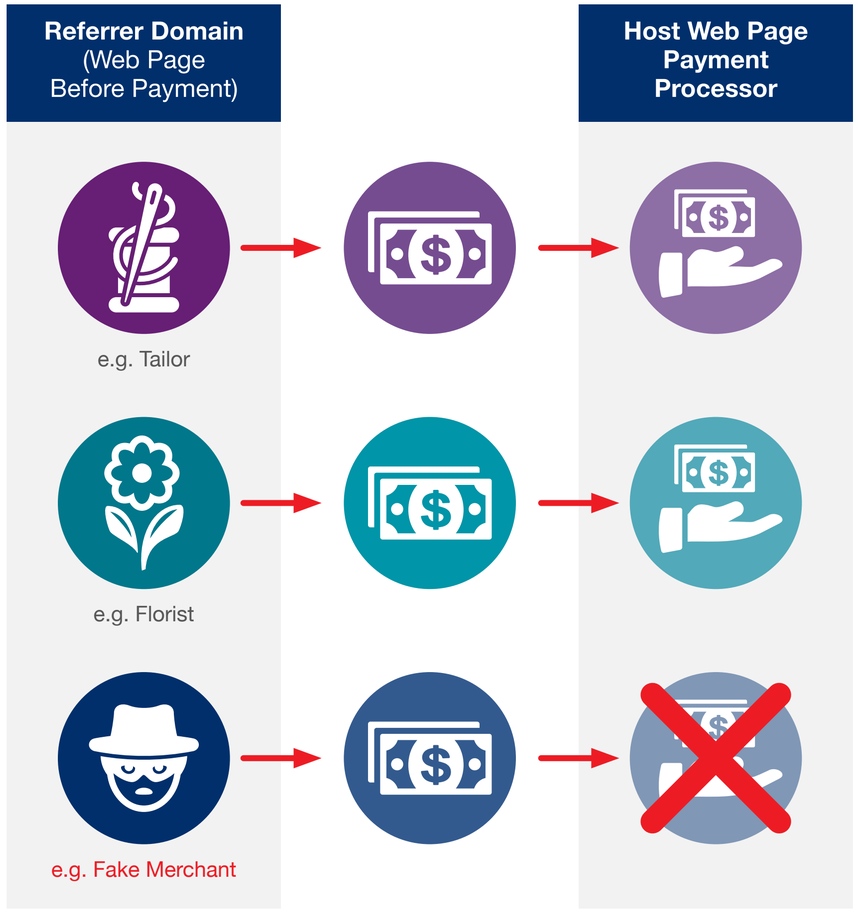
- Unauthorized merchant selling illegal or restricted goods

Method:

- Fraudster is masquerading as a legitimate or approved trader in order to continue to run an illegal or restricted online business, duping the payment processor into accepting its business

Detecting Fraudulent or Unauthorized Merchants:

- This payment processor was being targeted by a number of unauthorized merchants
- One of the attributes that the Digital Identity Network collects during an online transaction is the referrer domain, which gives LexisNexis® Risk Solutions customers visibility into the web page a transacting user has visited *before* hitting the host web page
- In this case, the referrer domain attribute shows the payment processor which merchant site the customer is buying from, before they make a payment
- In the example to the right, the payment processor used the referrer domain attribute to detect an unscrupulous merchant who was selling illegal or restricted items



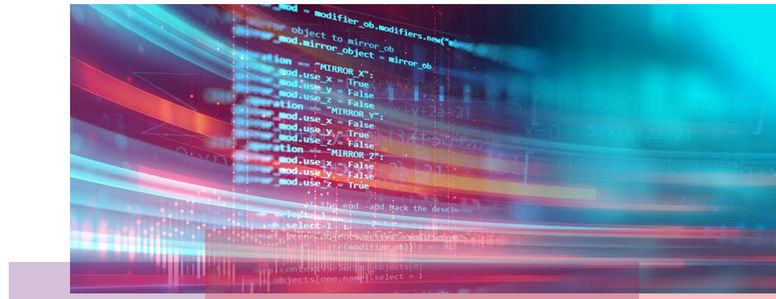
Spotlight: Personal Finance Company Becomes Target for Synthetic Identity Fraud

A personal finance company experienced a peak in bot activity across a two-day period in January 2019.

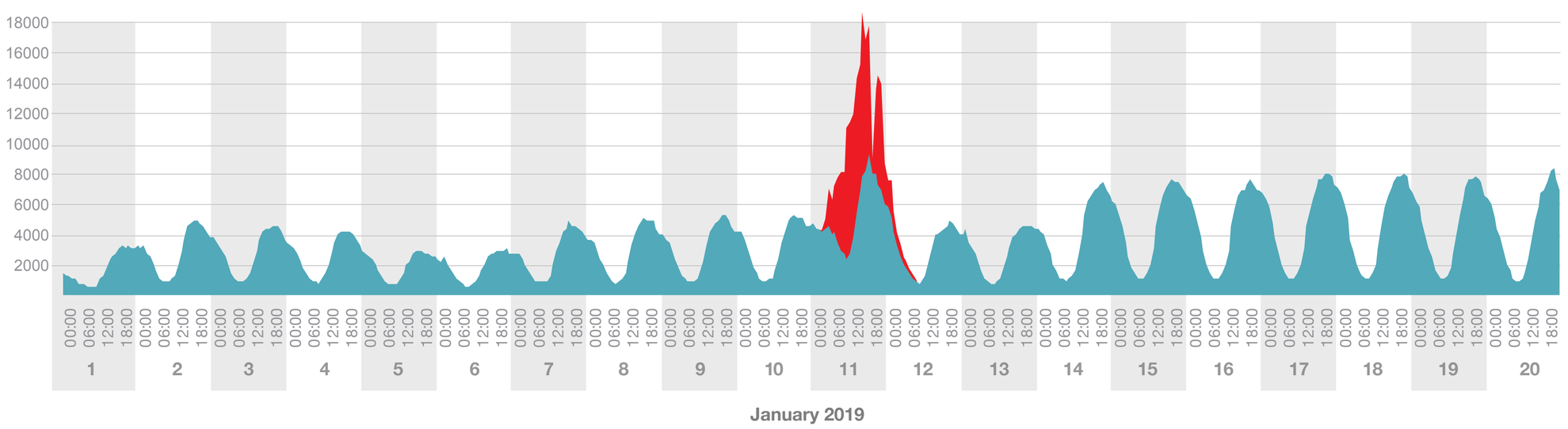
An automated bot was being used to create thousands of fraudulent new accounts using synthetic identity credentials, with small variations on the email domains.

At its peak, the bot attack was attempting to create approximately 12,000 new accounts an hour, significantly impacting business processes.

LexisNexis® Risk Solutions helped the personal finance company identify this traffic as fraudulent in near real time, preventing thousands of fraudulent new accounts from being created and potentially reducing hours of manual reviews.



Hourly New Account Creations at Personal Finance Company



The Media Industry's Role as Gateway for Digital Transacting Fuels Rise in New Account Creation Attacks

The media industry represents a key entry point to digital transacting; young adults, or consumers from growth and emerging economies new to online interactions, often create their first digital footprints by signing up to social media and content streaming sites.

This is reflected in the growth of new account creations, with the Digital Identity Network recording a higher proportion of new account creations in media than in any other industry.

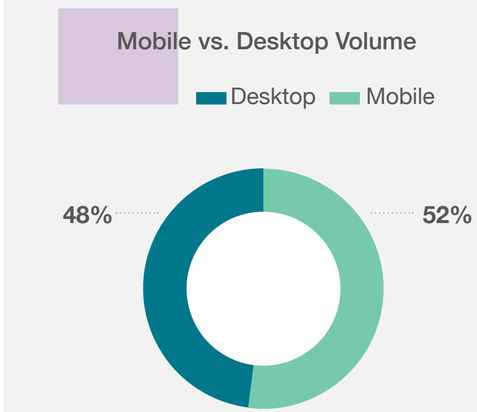
New media accounts are, however, at high risk of attack; around one in six new account creations is classified as an attack. These have grown 11% year-on-year, rising to 25% for mobile new account creations.

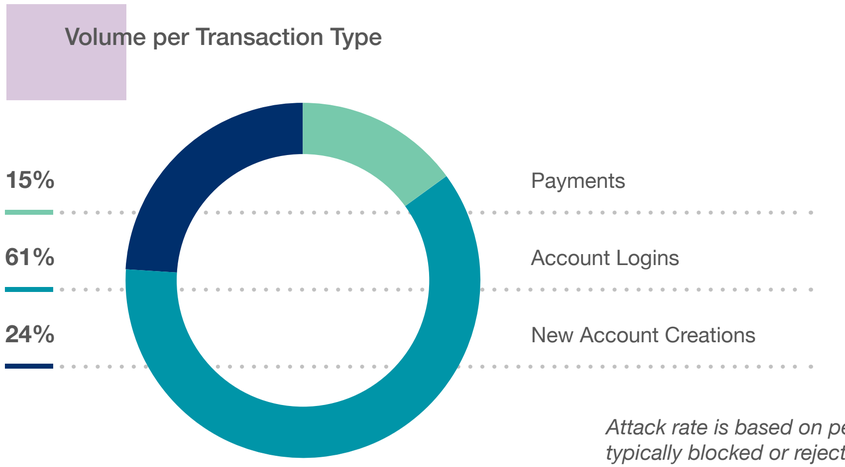
Attacks targeting the media industry originate from a diverse list of countries. Larger economies such as the U.S. and the UK rank alongside emerging economies like Colombia, Mexico and Brazil.

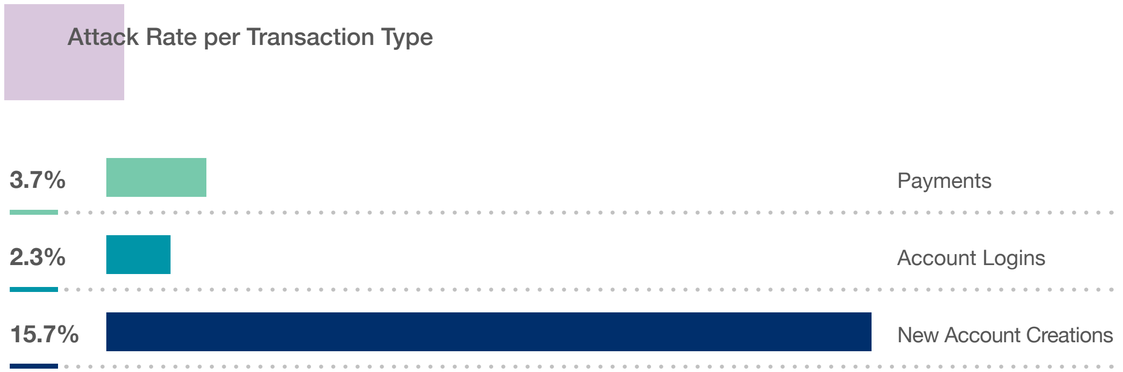
The Philippines, however, has climbed 19 places in just one year to join the rankings as a top attacking country targeting the media industry. The Philippines swift rise in the rankings is mainly due to a number of identity spoofing attacks originating from the country, targeting a global media streaming provider. These attacks also contributed to the 13% year-on-year growth in identity spoofing attacks recorded in the first half of the year.

However, the media industry is also under attack from bots, with such attacks increasing 22% year-on-year.

Interestingly, the media industry has historically been more desktop-based but, perhaps with increasing consumer adoption of mobile streaming, the percentage of mobile transactions has increased 20% year-on-year.







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 real time depending on individual customer use cases.

Spotlight: Fraudster Attempts to Hide Credential Testing Attack with Small Payments to Global Charity

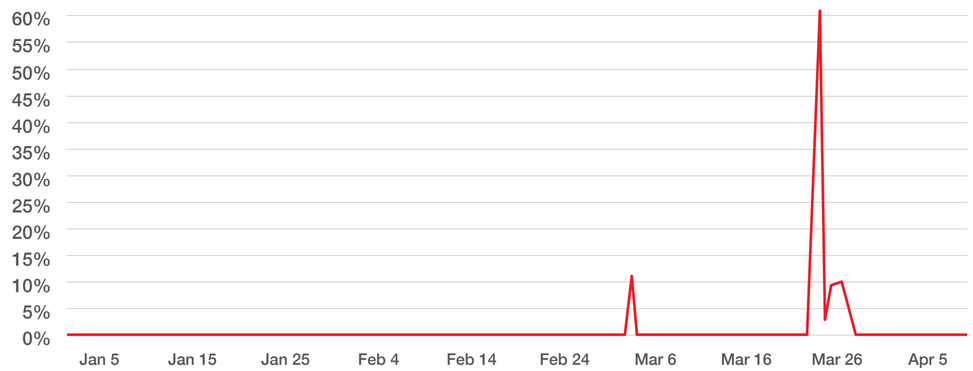
Fraudster:
- Fraudster from Iraq, with some attacks originating from the U.S. and Ecuador

Target:
- Global Charity

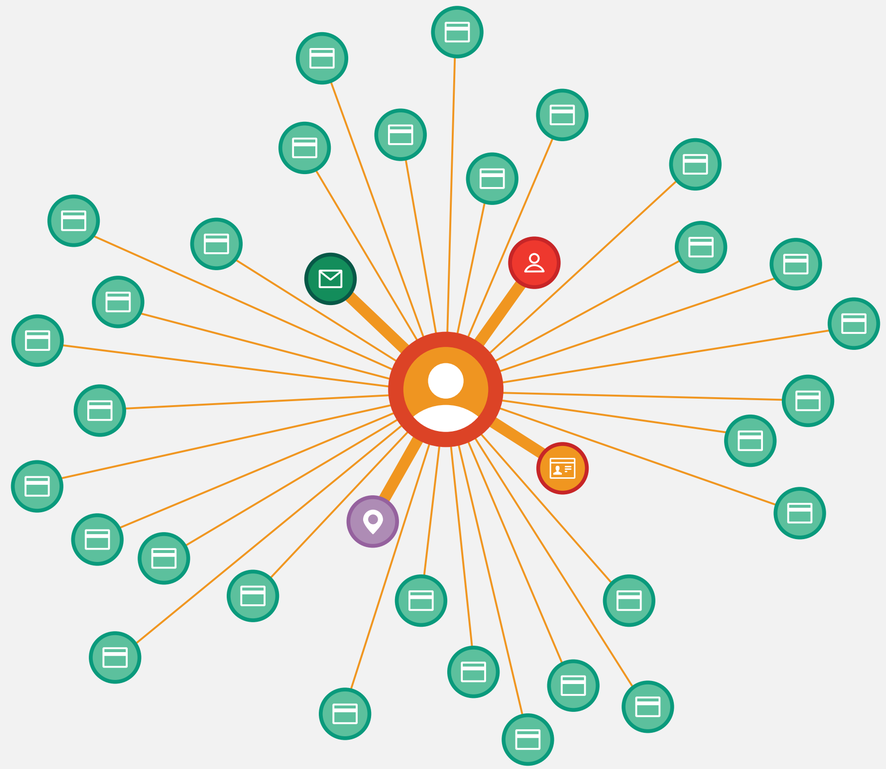
Method:
- Credential testing attack

Attack:
- Thousands of credit card credentials tested via small payments made to a charity
- Credit cards originated from Singapore, U.S. and Mexico
- Evidence shows that the fraudster, in one instance, used the same name, address, account name and device with 74 different credit cards.

Percentage of Payments Coming from Bots for a Charity Organization



Multiple Small Credit Card Payments Coming from One Fraudster



LexisNexis® RISK SOLUTIONS

Gaming and Gambling Sees Fraudsters Up Their Stakes in Search of Lucrative Bonuses and Fraudulent Payments

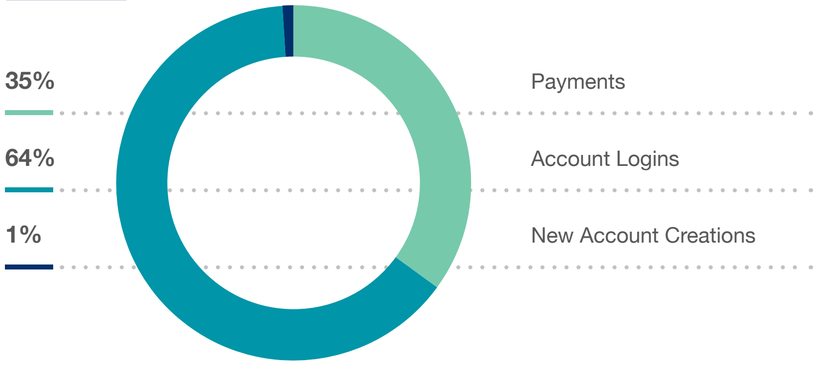
The gaming and gambling industry has undergone a rapid digital evolution, with brick and mortar casinos displaced by a plethroa of mobile and online gaming and gambling companies. Gaming has evolved beyond simple roulette / poker games, to near real-time, in-game betting. As the competitive field in gaming and gambling becomes more crowded, bigger jackpots, better odds and more lucrative bonuses are designed to attract new (and retain existing) customers. However, cybercriminals are also looking to win big, targeting accounts with stolen identity credentials in order to exploit free bonuses, or takeover genuine customer accounts and make fraudulent payments.

LexisNexis® Risk Solutions transactions in gaming and gambling follow a similar pattern to those in financial services, with both industries in the midst of regulatory change and undergoing transformation driven by the widespread adoption of in-game betting / gaming via mobile devices. Both industries experience high volumes of account logins and payments transactions, as you would expect from an industry driven by placing bets.

Mobile also facilitates this high volume of logins, as customers are able to check accounts on the move, whilst watching sporting fixtures, to make timely bets and transfer winnings.

Account creations and payments remain the most targeted transactions in gaming and gambling, with fraudsters targeting new account creations in order to exploit free bonuses. Logins are the least targeted transaction overall, suggesting that operators are perhaps choosing to block high-risk transactions at the payments stage, which represents the true moment of risk for both customers and the gambling operator in question.

Volume per Transaction Type



Attack Rate per Transaction Type

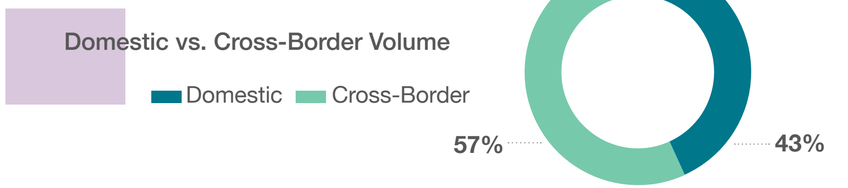
Attack rate is based on percentage of transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically and in real time depending on individual customer use cases.

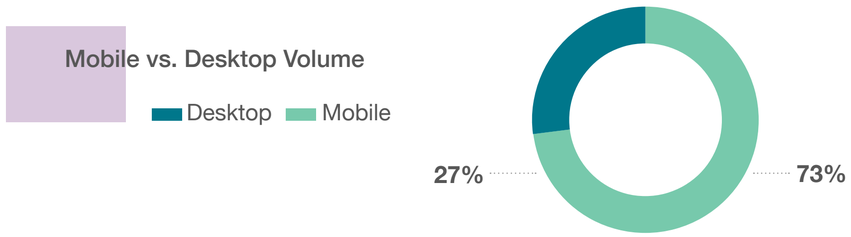
Gaming and Gambling Industry is Winning Big with Mobile and Cross-Border Transactions

In the first half of 2019, the Digital Identity Network recorded 57% of all gaming and gambling transactions as cross-border traffic. The high volume of cross-border traffic is indicative of the global customer base enjoyed by operators, although such traffic does present a number of challenges for operators already in the midst of regulatory change.

Cross-border traffic can make it more difficult for operators to verify the true location of a transacting gamer. Problem gamblers or those who live in regions that restrict or ban gaming and gambling are further adding to this problem, often using VPNs or IP spoofing to try and obfuscate their true location.

73% of all gaming and gambling transactions now originate from a mobile device, outpacing the industry-wide 62% seen during the first half of 2019.





Spotlight: Fraudster Masks Location to Target European Gambling Operator with Credential Testing Attack

Fraudster:

- Fraudster from the Ukraine

Target:

- European Online Gambling Company

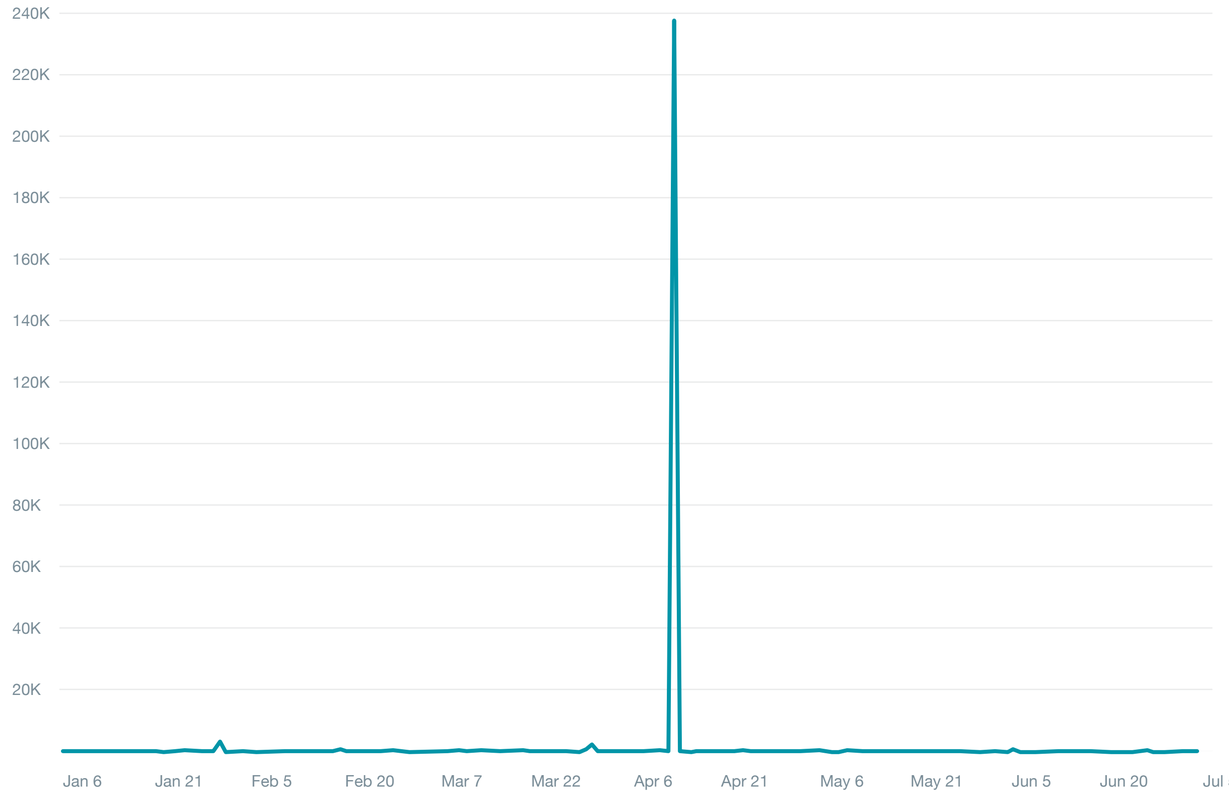
Method:

- High velocity credential testing and account takeover attacks

Attack:

- The fraudster attempted to login and takeover genuine customer accounts through testing numerous stolen credentials, such as name, email, telephone, address and password.
- The fraudster tried to mask their location by spoofing their IP address, with transactions appearing to originate from multiple locations from across the world.
- The fraud was detected by identifying that the transactions came from the same device and location, with the IP address of the device indicating that the fraudster was in the Ukraine.

Daily Attacks on European Gambling Operator



Conclusion

Mobile has been no less than revolutionary in terms of the global digital economy and its impact on businesses and consumers. Mobile will, however, continue its revolutionary march; 5G networks will fuel new operational models, architectures and service delivery models. 5G may also, however, create new opportunities for fraudsters trying to exploit weaknesses and target devices which may be without robust security defences – indeed, fraudsters could gain entry to homes via a raft of IoT devices, for example. There is also concern that fraudsters will target data in transit, hijacking devices to steal customer credentials, capture credit card numbers and infect networks with malware.

While the Digital Identity Network continues to demonstrate the benefit of strong mobile penetration across markets and geographies, organizations must ensure that the volume shift to mobile transacting does not open up vulnerabilities to cybercriminals looking to capitalize on this change in customer behaviour.

Over the course of the last five years, the Digital Identity Network has also seen a complex evolution of global cybercrime, with the emergence of sophisticated networks of fraud operating across organizations, industries and use cases. Cybercrime has emerged as an industry in its own right and, according to Cybersecurity Ventures will be one of the biggest challenges that humanity will face over the next two decades.

These criminal networks are now mirroring legitimate enterprises; ‘finance departments’ deal with the laundering of money, whilst ‘procurement’ enlists money mules and ‘engineering’ develops cutting-edge attacks to bypass the latest advances in cyber defences. This growth industry is set to cost the world over $6 trillion annually by 2021, according to the same Cybersecurity Ventures report.[1]

[1]Cybersecurity Ventures, 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

But how do you defend against these increasingly sophisticated networks of fraudsters? Single point solutions are no match to this networked cybercrime, with fraudsters adept at masking themselves as legitimate and trusted customers in order to maximize monetary gain and minimize detection. The most robust solution to this growing problem is a layered defence of fraud, identity and authentication capabilities, executable in near real time, and across the entire customer journey. This relies on uniting world-class digital identity intelligence, physical identity and authentication capabilities that can help businesses meet regulatory requirements, streamline the customer experience and detect complex and evolving fraud.

Glossary

Regions

North America region includes: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, Bonaire, British Virgin Islands, Canada, Cayman Islands, Costa Rica, Cuba, Curacao, Dominica, Dominican Republic, El Salvador, Greenland, Grenada, Guadeloupe, Guatemala, Haiti, Honduras, Jamaica, Martinique, Mexico, Montserrat, Nicaragua, Panama, Puerto Rico, Saint Barthelemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Sint Maarten, Trinidad and Tobago, Turks and Caicos Islands, U.S. Virgin Islands, United States.

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, typically through a spoofed location, to create a new account to 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 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: Hackers 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 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 (such as SMS out-of-band authentication messages) 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 use slow traffic that not only appears legitimate but also bypasses any triggers set around protocols and 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 unite 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
- Consistently 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

Data Processed and Analyzed

From the 16.4 billion transactions processed globally January-June 2019, LexisNexis® Risk Solutions uses subsets to conduct detailed analysis.

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 (277 million) based on the profiling data within our Digital Identity Network.
- For the sophisticated attacks, LexisNexis® Risk Solutions considers a subset of 13.1 billion of the 16.4 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.

For more information:
risk.lexisnexis.com/FIM-EN

Americas:
+1 408 200 5755
+1 800 953 2877

EMEA:
+44 203 2392 601

APAC:
+61 2 9411 4499

LexisNexis®
RISK SOLUTIONS

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, ThreatMetrix IDTM LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time. ThreatMetrix is recognized as the sole Leader in the 2017 Forrester Wave™ for risk-based authentication. Learn more at www.threatmetrix.com.

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 www.risk.lexisnexis.com, and www.relx.com

LexisNexis®
RISK SOLUTIONS