ThreatMetrix®

Q4 2016 CYBERCRIME REPORT

160 W Santa Clara St
San Jose, CA, 95113
United States

Telephone: +1 408 200 5755
Fax: +1 408 200 5799
sales@threatmetrix.com

Alisdair Faulkner

Chief Products Officer

We started the year focusing on the digital transformation strategies that organizations needed to prioritize in order to keep pace with the fast-evolving digital world. As 2016 draws to a close, digital users are hardly even aware of the lengths that some businesses have gone to to safeguard streamlined online access to goods and services.

Consumers have now simply come to expect this as the norm: friction-free access to the digital sites they love, that fits in to the ebb and flow of their daily lives without noise or fanfare. So much so that many digital interactions have now become almost habitual, at times not even mandatory but just something users do as part of their daily routine. Get up, check the news channels, scan social media, review train disruptions, monitor bank balances, select groceries. We hardly give these a second thought.

The challenge for digital businesses in 2017 becomes not so much prioritizing digital transformation, but maintaining the established relationship with trusted users to ensure the consistent level of interactions that they expect. We live in a highly digital, intricately connected world where lack of interaction is simply not an option.

Mobile transactions continue to grow as users favor the ease and mobility of transacting wherever and whenever they choose. And when businesses get this mobile experience right - with a slick user experience and minimal friction - they profit considerably more than the digital laggards.

FinTechs too are disrupting the market with product innovation driven by real time data, cloud-based solutions and Millennials hungry for change. Gone are the days when high street banks or insurance giants monopolized the financial services market; e-lenders crowdsourcing loans and buy-and-go insurance companies are slotting in to the gaping crevasses that some of the big players simply can't fill.

This quarter we've also seen some particularly interesting holiday trends: holiday season shopping is no longer the nail-biting 100m sprint, but rather the five-day test match; exploding out of the confines of traditional key days to be a year round phenomenon, with multiple busy online shopping periods. Consumers are constantly on the lookout for the best deals, and retailers are attempting to maximize transaction volumes and basket sizes year-round.

The worrying thing for digital businesses, however, is that hashed passwords or encrypted data mean very little to the cybercriminals of 2017. Fraudsters are continually one step-ahead, concocting near perfect identities from the digital detritus that companies and indeed individual users are giving up. It is identity, not passwords or payment details, that is the cybercrime currency of 2017: near perfect, yet terrifying, simulacrums of you and I that can be used to open new accounts, hack into existing ones, and monetize fraud attacks.

On the plus side, however, successes in the cybercrime war are having an impact on overall attacks, particularly as organized criminal networks are able to control huge armies of fraud attacks: bring down the network and the workers tumble. One such success was the bringing down of Avalanche, a criminal syndicate involved in phishing attacks, money mule schemes, and ransomware. This is potentially one of the reasons we have seen an overall decline in automated bot attacks this quarter.

Recap and Key Trends

Criminal Franchise in a Box: Cybercrime is more automated, organized and networked than ever before, evolving way beyond hipsters wearing hoodies and hacking from the basement. The growing sophistication of cybercriminals is evident in the evolution of attacks and the use of advanced tools, such as malicious programs, that allow criminals without technical skills to deploy computer ransomware or perform video or audio eavesdropping with a mouse click. This extends the reach of global cybercrime from the technical few to the non-specialized masses, scaling its growth exponentially. However in turn as the bringing down of the botnet Avalanche has shown, removing such networked rings can have a real impact on fraud volume globally.

Global Volume: Transaction volume is no longer regional, or even confined to country borders, but has rather exploded cross-border as the global village economy has really taken root. However, cross-border transactions are riskier than domestic ones; organizations must look for better ways to authenticate their user base on a global rather than regional scale.

Shared Economy: The concept of online communities has exploded across industry groups, from crowd-sourced loans to travel reviews, charitable giving and online marketplaces. What such platforms rely on, however, is an inherent currency of trust. Users must be able to review, give and buy with confidence to avoid destabilizing the reputation of such businesses.

Account Validation Attacks:
Identity is the cybercrime currency of the future, allowing fraudsters to monetize attacks through sophisticated account takeovers, fraudulent new account creations and fake payments. 1 in 10 new account creations are now rejected, illustrating the widespread and pernicious use of stolen identity credentials.

Identity Testing: Cybercriminals are preying on industries with the least digital sophistication / companies that are less likely to block payment transactions to test stolen identity credentials: namely nonprofits. Via numerous small value payments fraudsters can quickly isolate validated stolen credit cards and use these to make a high value purchase elsewhere online.

Digital Mobility:
At the end of 2015, around a third of transactions were mobile. In 2017 this will rise to more than half – a statistic we already see in financial services. Static users transacting on a stationary device is a thing of the past. Organizations must align authentication and identity verification with a constantly mobile user base.

Report Overview

The ThreatMetrix Cybercrime Report: Q4 2016 is based on actual cybercrime attacks from October – December 2016 that were detected by the ThreatMetrix Digital Identity Network (The Network) during real-time analysis and interdiction of fraudulent online payments, logins and new account applications.

The ThreatMetrix Digital Identity Network provides visibility and insight into traffic patterns and emerging threats. The Network analyzes close to two billion transactions per month, over 44% of which originate from mobile devices.

These transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioral analytics.

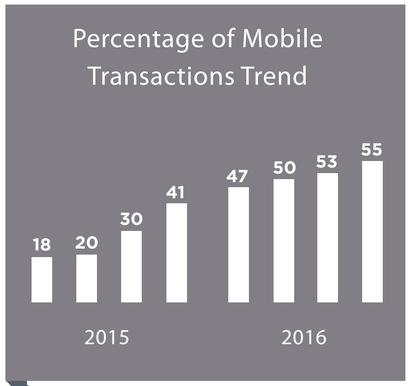
The Network and its real-time policy engine provide unique insight into users' digital identities, even as they move between applications, devices, and networks.

ThreatMetrix customers benefit from a global view of risks, based on these attributes and rules that are custom-tuned specifically for their businesses.

Attacks discussed are from "high-risk" transactions scored by ThreatMetrix customers.

> *The ThreatMetrix Digital Identity Network provides visibility and insight into traffic patterns and emerging threats. The Network analyzes close to two billion transactions per month, over 44% of which originate from mobile devices.*

Financial Services Key Trends for 2016



MOBILE **5.8X** DESKTOP **3.1X**

Number of times a week customers log in to their bank account

80M

Number of attacks using stolen or fake credentials

254%

Growth of account login transactions from mobile devices

55%

Percentage of FS transactions coming from mobile devices at end of 2016

125%

Growth of account creation transactions from mobile devices

250%

Percentage growth of FS mobile transactions year-on-year

THE EUROPEAN UNION

PSD2 continues to be a hot topic for European financial services providers while FFIEC mobile banking and payment guidance puts risk front and center in US.

EU Payment Accounts Directive comes into force in UK, opening up cross-border bank account provision to all EU residents.

Insider threats feature prominently in several high profile financial services breaches (Bangladesh bank heist and Tesco Bank breach).

ECommerce Key Trends for 2016

- Global village economy gains strength and popularity and merchants see higher volume of cross-border transactions throughout the year.
- Holiday season shopping has evolved from being confined to a particular day to include longer periods of deal-hunting and sustained transaction peaks.
- EMV migration has shifted payment fraud further online.

51%

Increase in blocked transactions year-on-year

44%

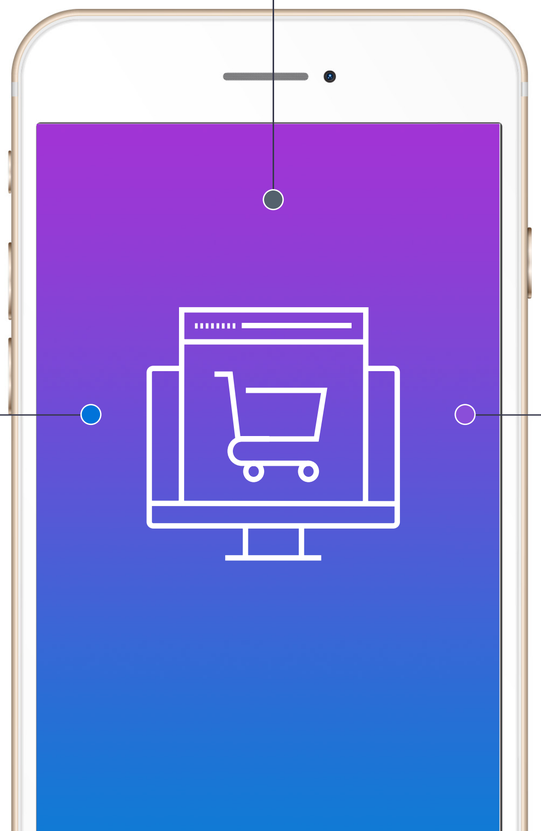
ECommerce transactions have strongest cross-border footprint of all industries

2X

Average ticket size for rejected transactions is twice as high as for good transactions

90%

Of dailly traffic attributed to Bot attacks for some key retailers



57%

Increase in volume of rejected payment transactions

134%

Growth in rejected account creation transactions

35%

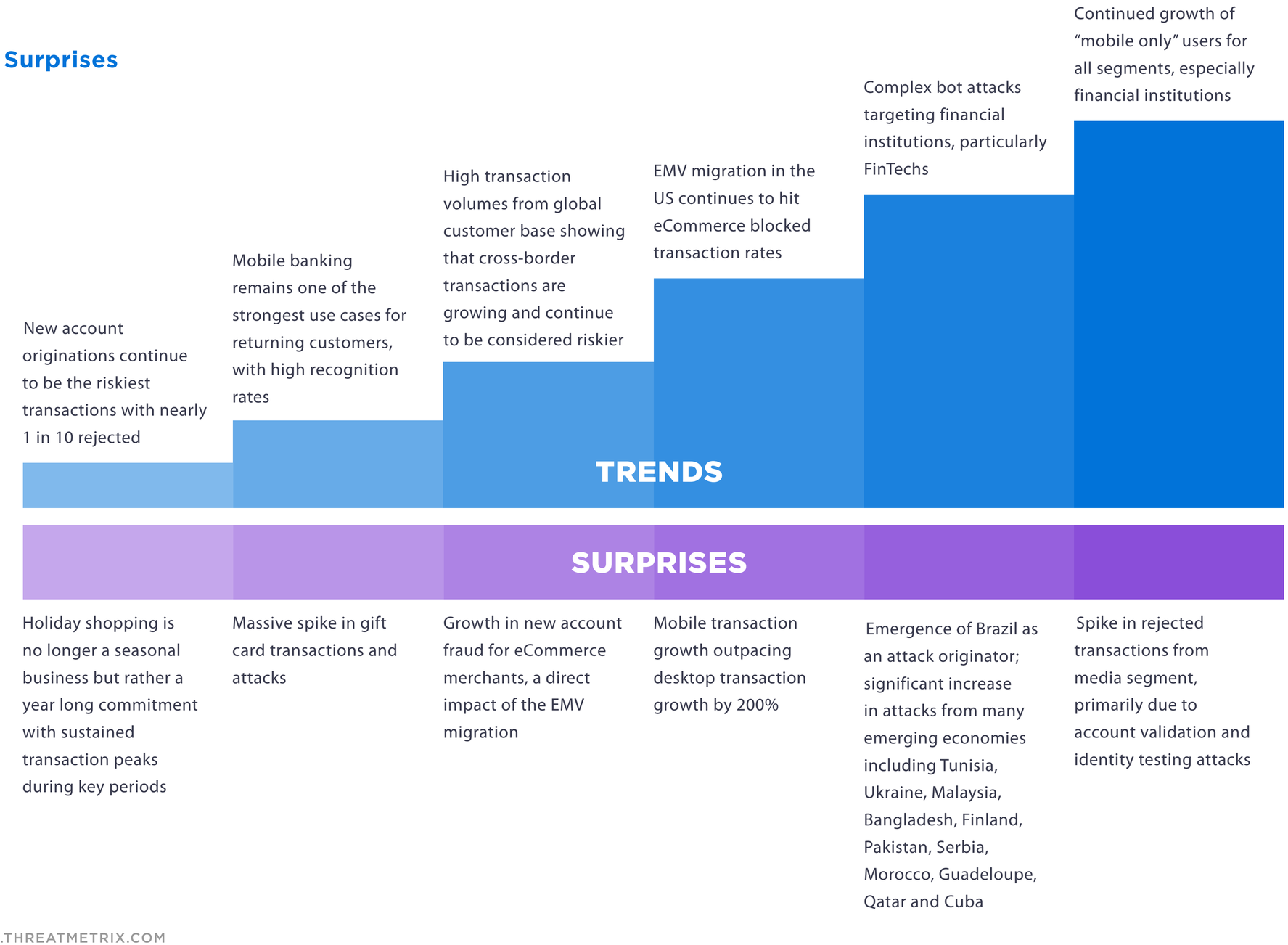
Percentage that mobile transaction growth outpaced desktop transactions

Q4 2016 Cybercrime Report – Key Highlights

ThreatMetrix analyzes transactions from top organizations across industries. Trends observed are representative of the key market trends:

- Q4 2016 represented the biggest digital quarter for the ThreatMetrix Digital Identity Network
- 122 million attacks were detected and stopped in real time; more than 35% increase over the previous year. Growth in attack outpaced overall transactions growth and the overall rejected transaction rate grew 15%, demonstrating the heightened risk levels
- The impact of recent organized cybercrime arrests (specifically in relation to the Avalanche botnet) was visible in the reduced bot attack levels
- Digital authentication continues to be one of the biggest use cases globally; however new account originations are growing fast across industries
- The theme of digital mobility features strongly in this report:
  - 45% of transactions now come from mobile devices, a 32% increase on the previous year
  - Mobile-only users have increased across all industry groups
  - Cross-border transactions are growing in prevalence; more than a quarter of transactions in the network are now cross border, indicating the importance of businesses using more than legacy rules to accept or reject global transactions

Trends and Surprises



Recognition is Key

Persona (device, identity, behavior) recognition by the ThreatMetrix Digital Identity Network ensures that businesses are able to effectively differentiate between trusted users and potential threats.

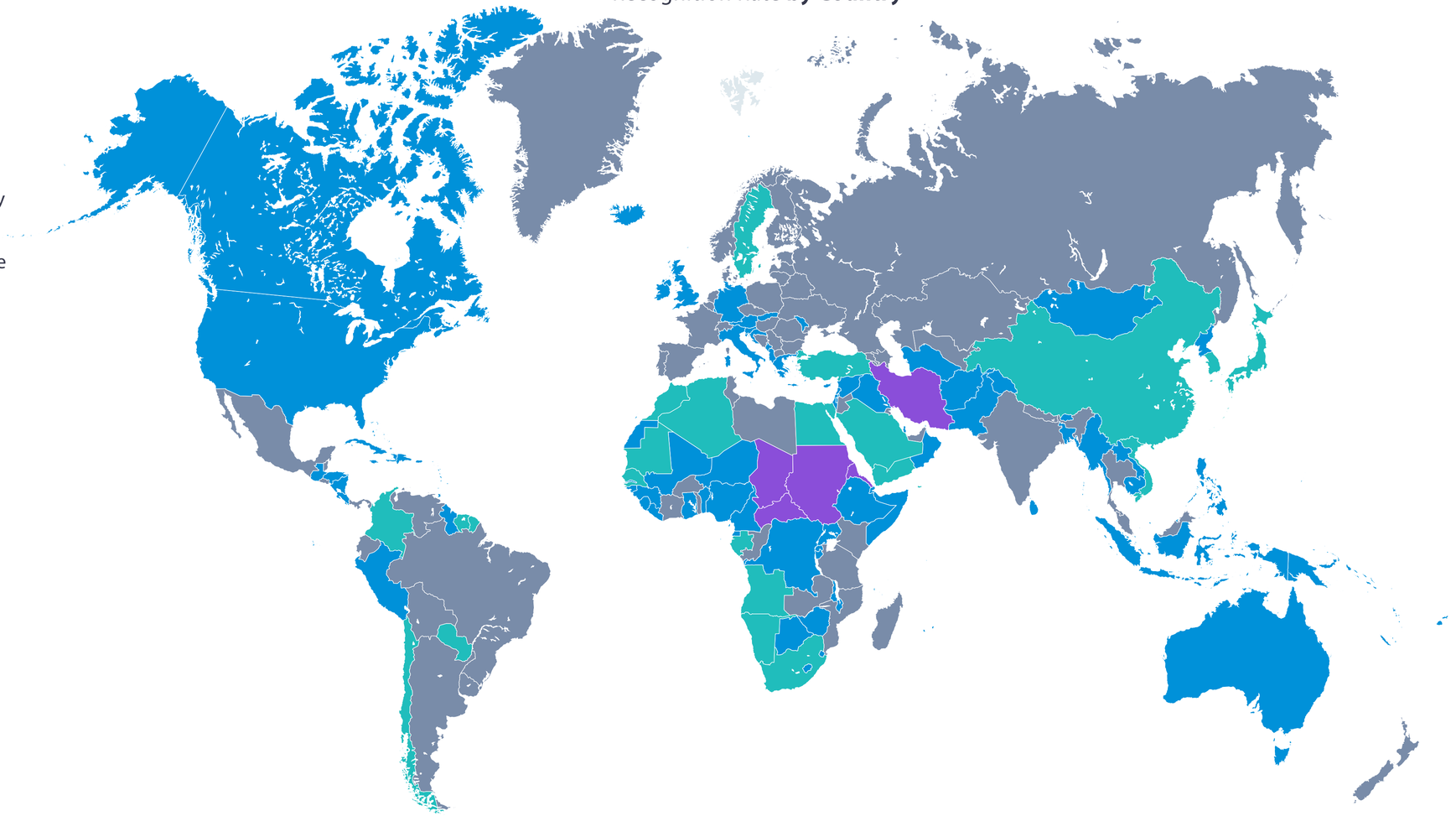
95 - 100%

90 - 95%

80 - 90%

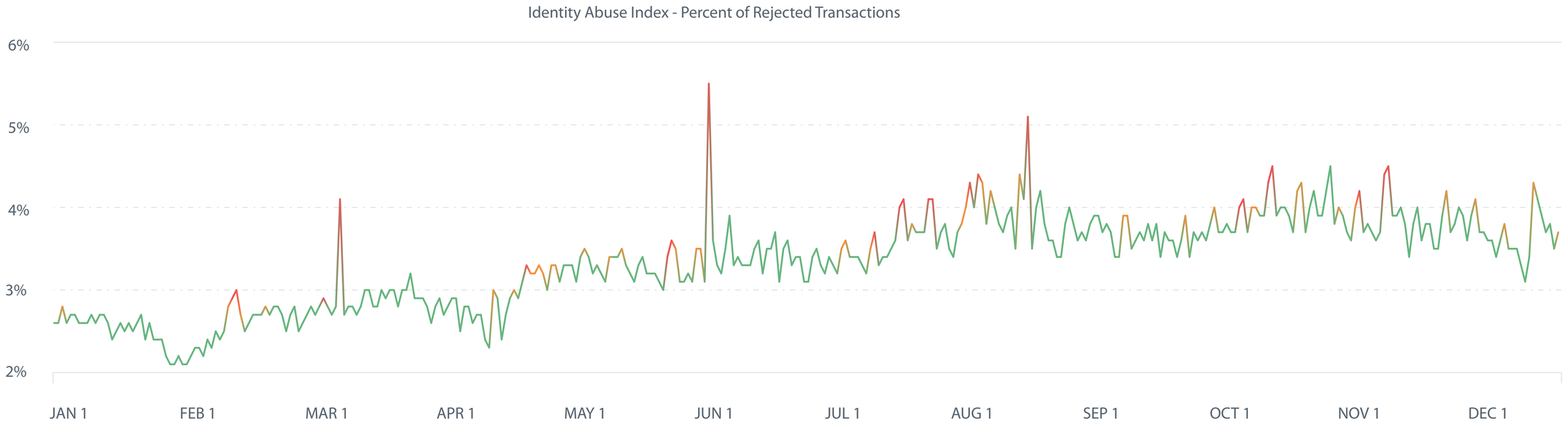
< 80%

Recognition Rate **by Country**



ThreatMetrix®

Attacks Continue to be Bigger, More Frequent and More Complex



2016 brought many new high profile breaches to light and the impact of these was evident in the continued growth of attacks on businesses across the globe. The end customer does not differentiate between identities breached from behind a network/ firewall or via an account compromise as the impact of the breach on their digital footprint is the same.

The identity abuse index shows numerous high level peaks throughout the year, indicating the sustained impact of global data breaches.

Companies are often quick to issue reassurances that stolen password data was hashed or payment credentials encrypted, but what is clear is that identity data is the critical currency in global cybercrime, as fraudsters piece together full and convincing identities which are then used to perpetrate large-scale attacks.

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

Low

Medium

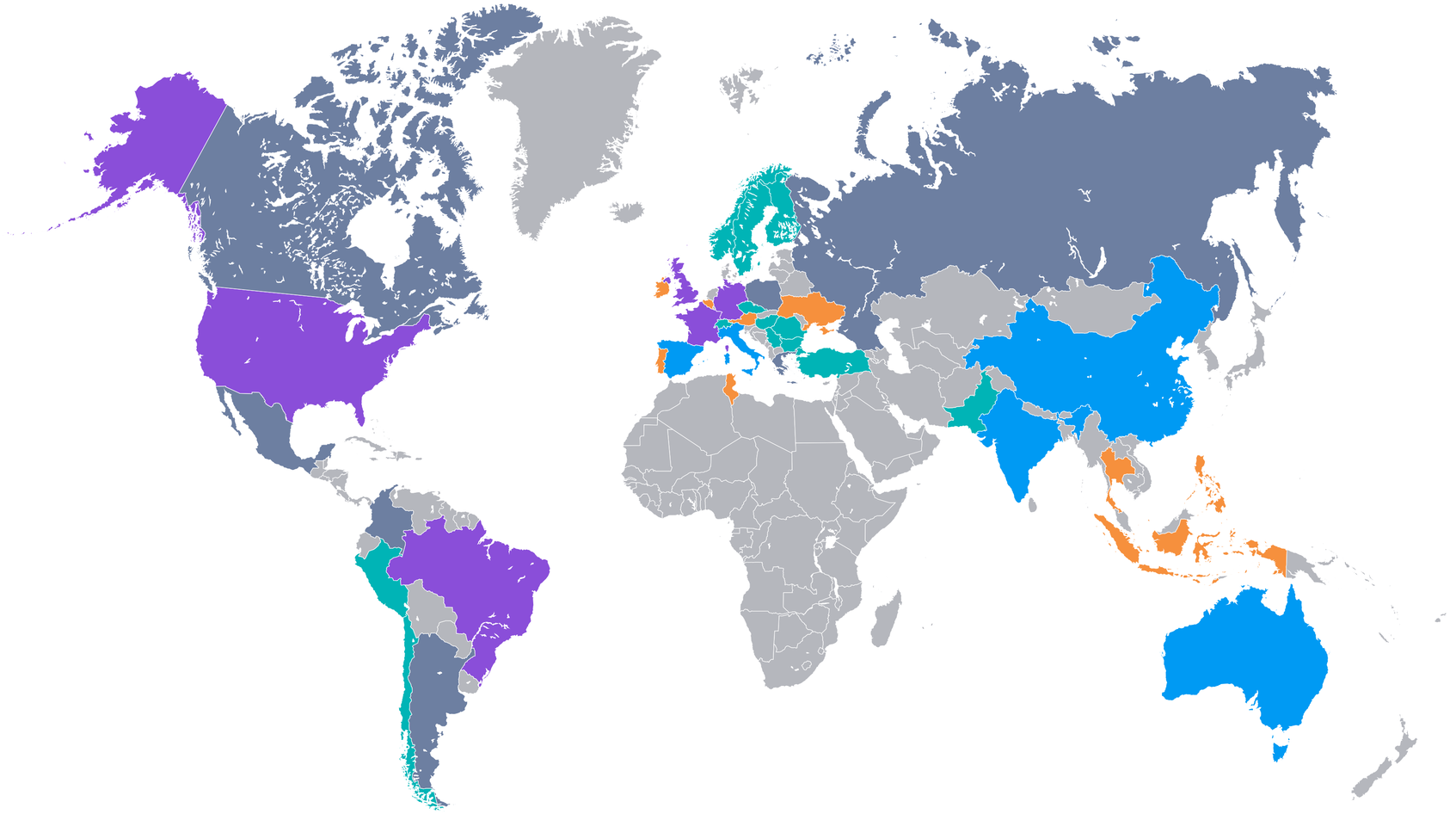
High

Attack Origins by Geography

Brazil, as well as some Central and Eastern-European are fast becoming some of the biggest attacking nations.

We are seeing strong attack growth in several emerging economies in the APAC region such as India, Qatar, Morocco and Tunisia.

This demonstrates the widespread trickling down of breached identity data to countries across the globe.



Based on total number of attacks detected by geography of origin.

Top Attack Originators and Attack Destination

The largest attacking nations generally target other similar economic nations: the strongest economies of US and Europe are targeting each other while the emerging economies such as Brazil are targeting attacks at other South American regions.

Attacks from UK

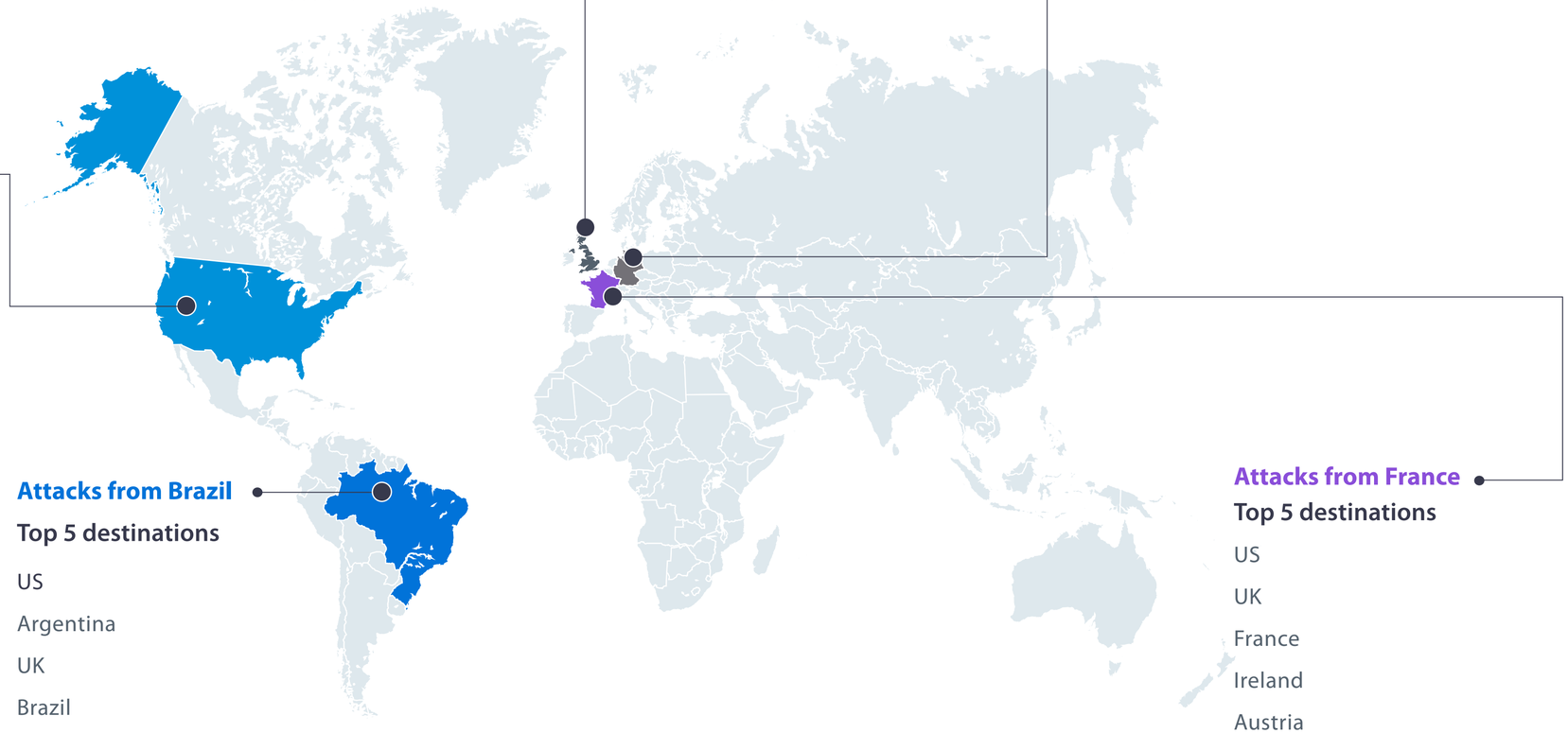
Top 5 destinations

US
UK
Ireland
Austria
Australia

Attacks from Germany

Top 5 destinations

US
UK
Germany
Austria
Ireland



Attacks from US

Top 5 destinations

US
UK
Canada
Australia
Austria

Attacks from Brazil

Top 5 destinations

US
Argentina
UK
Brazil
Colombia

Attacks from France

Top 5 destinations

US
UK
France
Ireland
Austria

Transactions Analyzed by Type

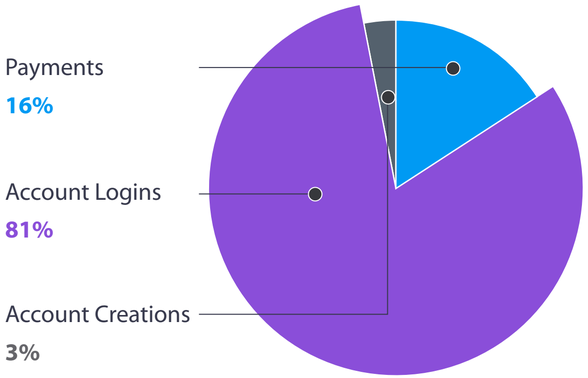
ThreatMetrix transactions span eCommerce, financial services and media sectors and cover the authentication, payments and account originations use cases. Logins and payments continue to be the biggest use cases as our customers deploy ThreatMetrix to authenticate user identities without impacting consumer experience.

This was the biggest digital quarter for the network with significant growth across segments. However growth in attacks outpaced the transaction growth by 15% as the continued impact of recent breaches and the EMV migration is having a greater and greater impact.

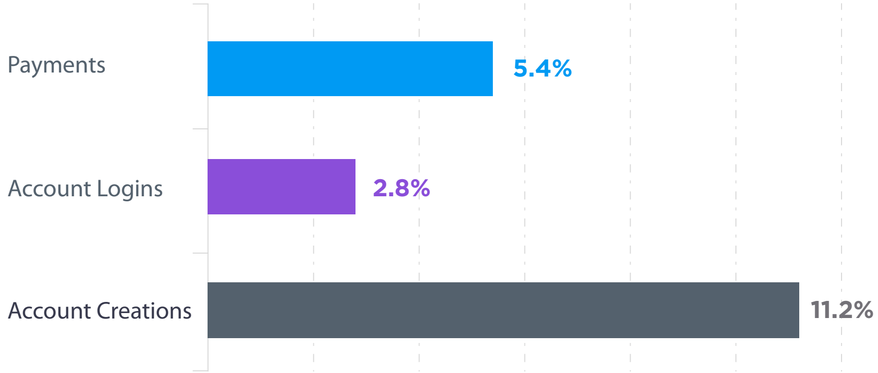
Attacks on new account creations went up 200% compared to the previous year. This large increase in account creation fraud is driven by the increased availability and low cost of stolen identities in the wild, harvested from massive breaches.

50% of transactions (65% mobile) come from financial services, primarily logins, driven by high consumer engagement and a high proportion of customers accessing services via their mobile phone / app.

Volume per Transaction Type



Reject Rate per Transaction Type



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.

Recognition Across Devices – New and Old

Online access allows digital consumers to interact with trusted providers more regularly than if they had to visit a physical branch or store. Users can share a much closer relationships with businesses and login to their accounts frequently. This creates a larger volume of transactions from repeat visitors and returning customers.

The Network continues to grow rapidly with hundreds of millions of new users and associated devices added each month. As more and more consumers are transacting online, the recognition rate is continuing to grow.

While the device recognition rate is highest for financial services companies and for transaction type "account login", as users are logging in on a regular basis to check their accounts, eCommerce recognition also continues to grow.

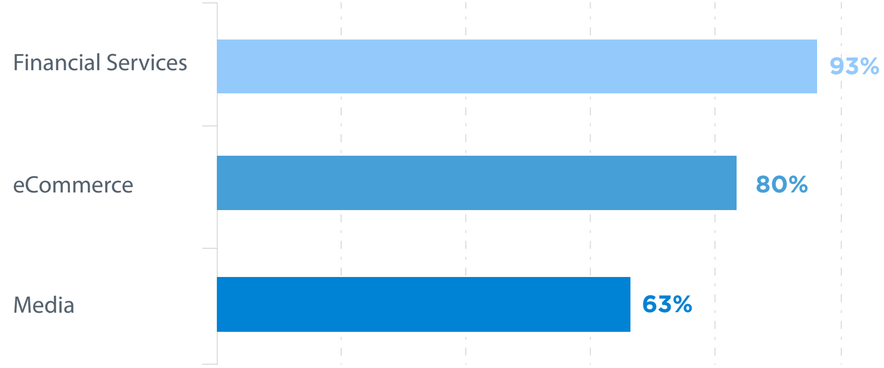
Holiday season sees a wide variety of transactions from both new and existing customers; despite this, ~80% of the transactions come from recognized devices and other aspects of a user's true digital identity are leveraged to authenticate users in real time, including location intelligence, online behavioral patterns and other anonymized personal information.

The recognition for mobile devices is around 93%. This higher recognition ensures that businesses are able to deliver a frictionless experience to their mobile users.

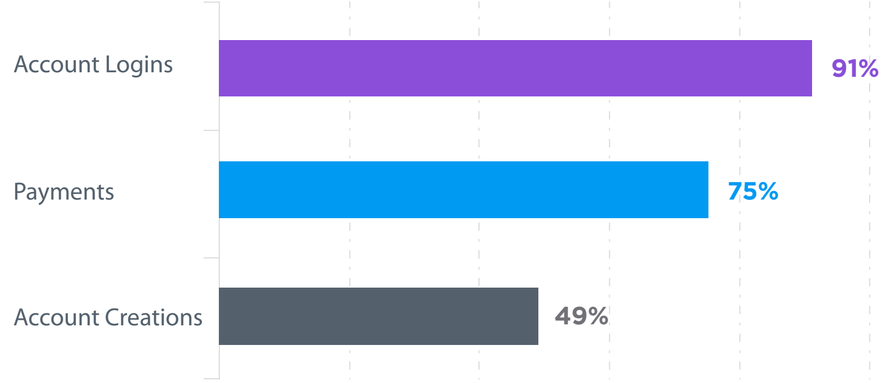
Note: *recognition rates plotted are the % of transactions where the device is a returning device to The Network*

> ***The higher recognition rate for mobile devices ensures that businesses are able to deliver a frictionless experience for their mobile users***

Device Recognition Rate by **Industry**



Device Recognition Rate by **Transaction Type**



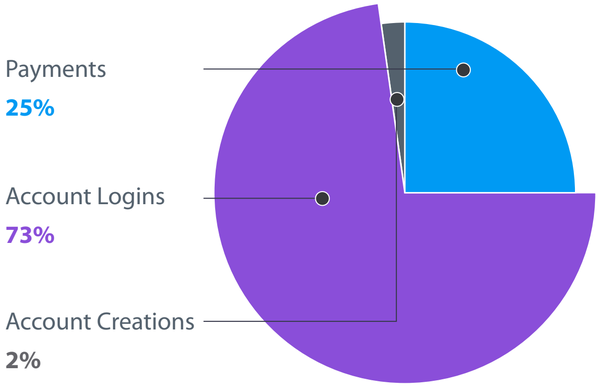
ECommerce Transactions and Attacks

This quarter saw a high level of attacks on eCommerce with more 75 million rejected transactions, representing a 35% increase over the previous year.

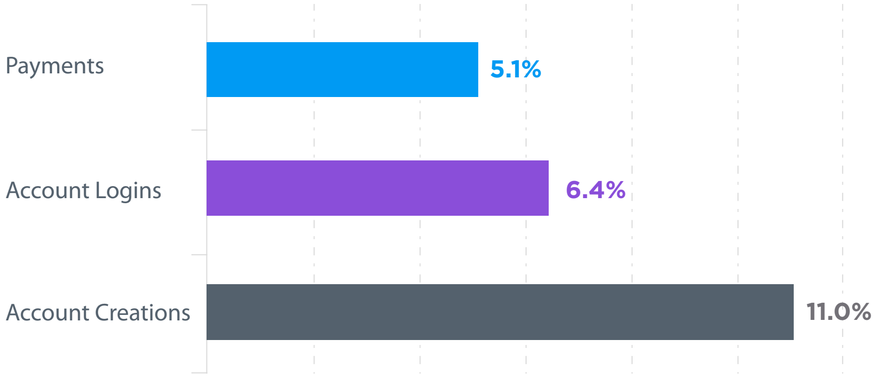
We are continuing to see the aftermath of last year's EMV migration, with fraud targeting eCommerce retailers growing at a rapid pace. Reject rates went up across all use cases, especially for new account creations as more and more fraudsters target eCommerce sites to test stolen credentials, particularly through automated bot attacks.

These attacks – which target user identities to access personal and payment information - are growing because it is much more lucrative to access a trusted credit card saved in a valid customer account than it is to attempt to re-use a stolen card that has a limited shelf life.

Volume per Transaction Type



Reject Rate per Transaction Type



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.

Holiday Shopping Goes Digital

Consumer activity intensified during the weeks leading up to to Cyber Monday as retailers began offering deals ahead of the peak shopping days.

However, many retailers lowered holiday forecasts as experts predict that holiday shopping is no longer a seasonal business but rather a year long commitment, with deals being sought outside the peak periods.

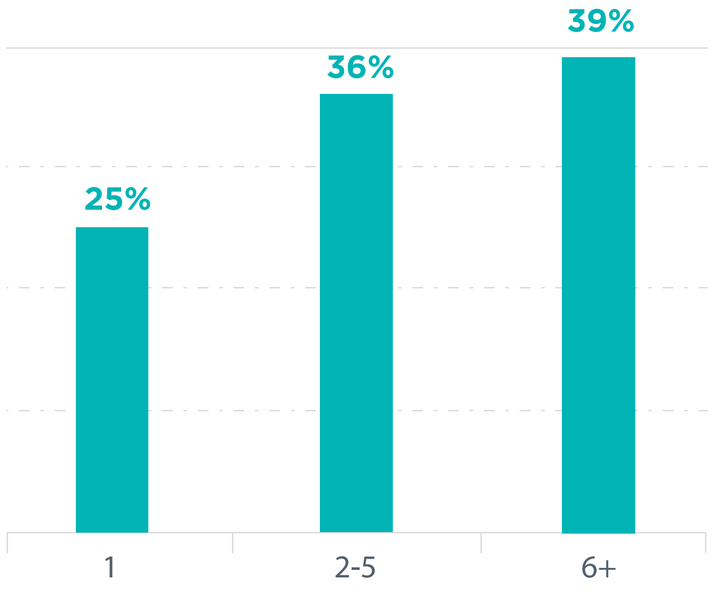
Of the 297 million transactions analyzed during this period, 75% of these came from consumers who were seen in the network more than once and 39% more than 5 times.

Recognition is key to stopping fraud without impacting customer experience and amidst huge shopping volumes, ThreatMetrix continued to recognize returning customers' Digital Identities.

By leveraging global shared intelligence across customers' digital footprints, ThreatMetrix was able to rate ~91% of the customers as low risk, which helped businesses deliver great customer experience without adding friction.

Percentage of Transactions

Thanksgiving Holiday Week



Number of times customer was seen in The Network

2016 Holiday Statistics – Usage and Growth

The secular trend to leverage digital channels continued through the holiday season. As with previous years, several trends emerged that demonstrate how connected devices and digital commerce has fundamentally changed consumer behavior and the face of holiday shopping.

The concept of Black Friday has become more of a sales tactic and has lost its relevance as retailers begin offering deals in the days leading up to and past thanksgiving. Despite this, The Network saw significant year-on-year growth for the top retailers from 2014-2016.

While transactions across the peak shopping days grew by over 25% year-on-year, the bigger growth happened on adjacent days, signifying the change in user behavior. There has been a perceptible shift from the feeding frenzy of Black Friday and Cyber Monday deals: these have evolved from being a time-constrained one-day event to the 3rd day of a leisurely 5-day cricket test match.

Digital commerce has enabled consumers to look for deals across retailers resulting in different retailers experiencing different peak shopping days. In addition, canny consumers are spreading their shopping across a number of retailers to take advantage of offers such as free shipping, meaning that ticket sizes are lower than average.

Gift cards are an increasingly popular choice, not just for gifting to loved ones, but also because they offer consumers the flexibility to pay now and buy later, or take advantage of deals later down the line.

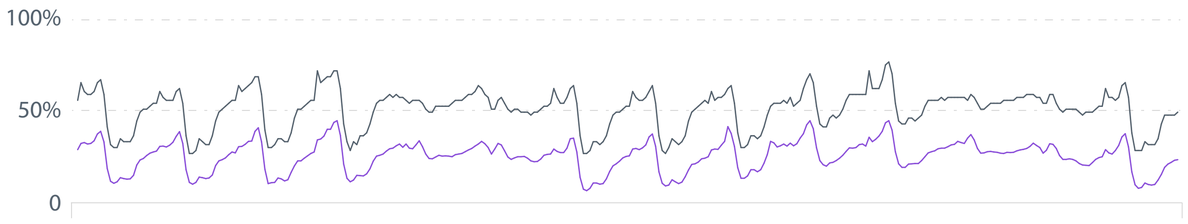
Consumers seamlessly moved between devices to browse for deals and shop online. Despite higher than average mobile volume during this period, (particularly at the weekend), desktop seemed to be the preferred connected device at peak shopping hours.

Peak transactions times were at 8-9PM which shows that shopping on these days is an afterthought rather than the prime event, fitting in to the ebb and flow of consumers' daily lives.

Despite the shift in consumer shopping behavior in the US, the concept of Black Friday and Cyber Monday have become a global phenomenon with increase in cross border transactions during peak shopping days.

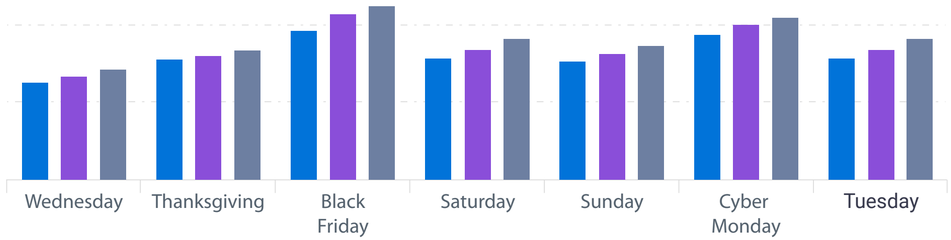
Hourly percentage mobile transaction 2015 vs 2016 - All industries

(10 days before Thanksgiving up to Cyber Monday) 2015 2016



Transaction Volume Thanksgiving holiday week

Top retailers 2014 2015 2016



The Rise in Popularity of Gift Cards

One of the big trends emerging this holiday season is the increase in gift card sales as shoppers are giving more gift cards as presents, satisfying last minute shoppers, pay now, buy later consumers and hard-to-buy-for friends.

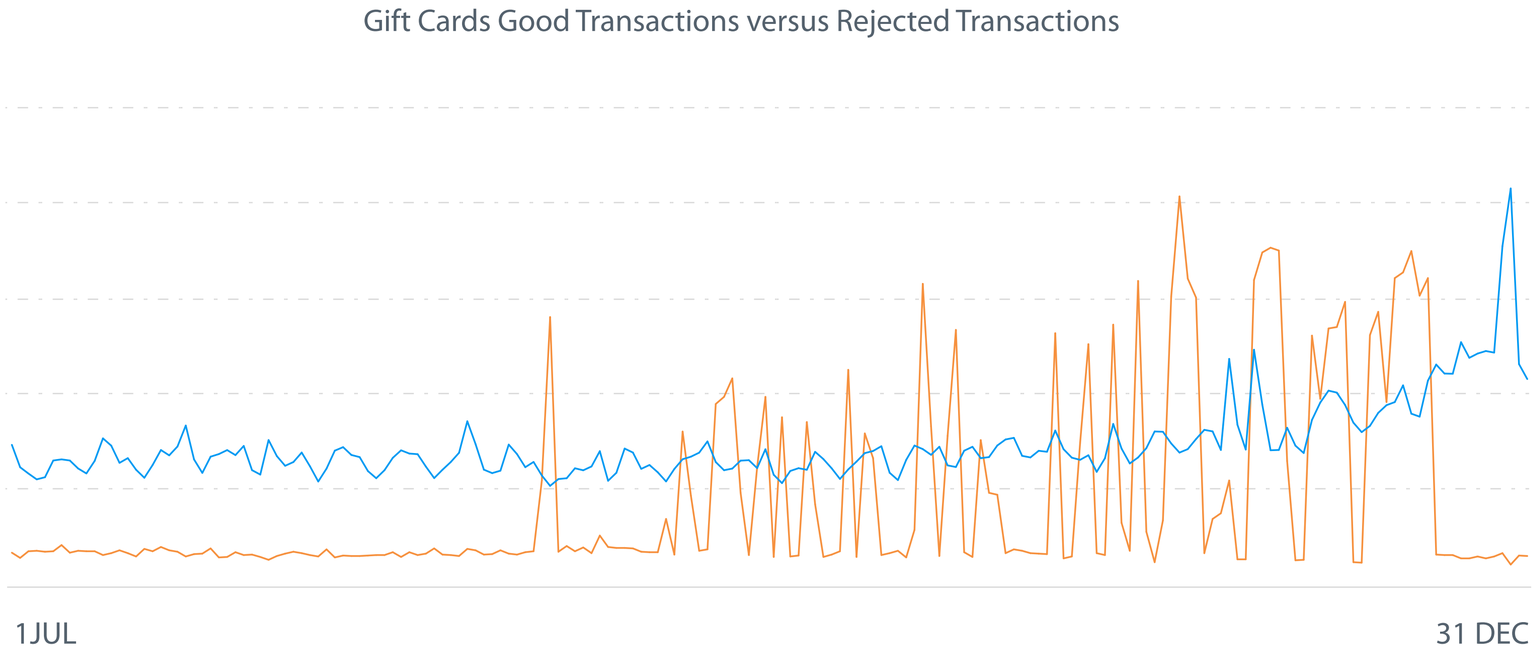
This is good news for businesses as gift card users tend to spend over and above the monetary value of their card, leading to higher sales revenues.

This has also opened up a large online market in gift card trading, with gift card marketplaces allowing people to buy and sell unused or unwanted cards.

With gift card sales estimates at $24.81B this holiday season1 (up from $18.48B last year), it is not surprising that fraudsters are also seeing opportunities for gift card fraud, attempting to dupe both unsuspecting customers and businesses*.

The Network saw large transaction spikes around the holiday season, as well as in the run up to Christmas. However, this also coincided with several sustained spikes in rejected transactions as fraudsters used bots to try and hack into gift card marketplaces.

*NRF data



Gift cards offer fraudsters the perfect opportunity to quickly monetize a stolen credit card, selling them on for cash at online auction sites and elsewhere. In addition fraudsters are selling used, counterfeit and fraudulent gift cards and even overstating their value to trusting consumers.

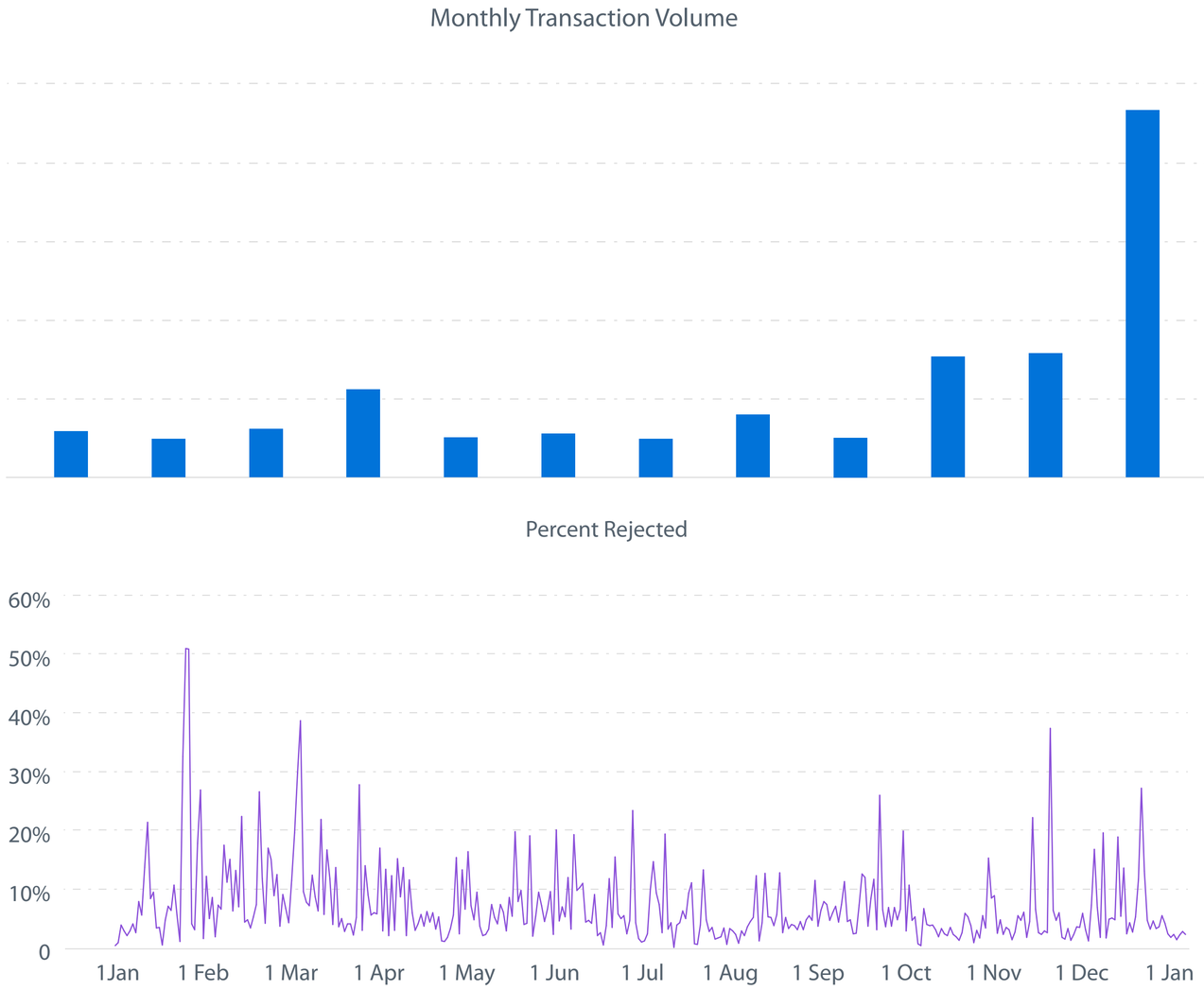
Charities - A Seasonal Business

Whiles charities work throughout the year to drum up monetary support, they experience very marked seasonal peaks and troughs in donations:

- The Tuesday after Thanksgiving is often referred to as "Giving Tuesday" in the United States and is intended as a global day of charitable giving at the start of the year-end holiday season.
- Over 35% of total charitable giving happens in December.

This seasonality, along with huge variations in the donation amount, makes charities across the globe especially vulnerable to fraudsters looking to test identities obtained through the dark web.

ThreatMetrix detected a series of transactions aimed at testing payment credentials. These $5 payments with stolen credit cards are designed to test the validity of these cards at the expense of the charities before using them elsewhere online to make a high value purchase.



CASE STUDY

Vantiv Stops Giving Tuesday from Becoming Fraud Tuesday

The Problem

Vantiv has a sizeable number of customers in the nonprofit sector: several were experiencing a rise in identity testing attacks.

These organizations typically minimize any barriers to donate, so sign-up procedures for new accounts and payments are as simple as possible.

This simplicity also appeals to fraudsters wanting to test stolen identity / credential data without the risk of detection.

These nonprofits were being actively targeted by fraudsters attempting to make small value payments (typically between $1-$5), testing the validity of stolen credentials before moving onto higher value purchases elsewhere.

Successful attempts were the gateway to big ticket items on other sites.

These attacks were happening extremely quickly and were hard to detect. They were also a significant drain on very limited resources and were increasing the volume of chargebacks and fees.

The Solution: Vantiv Fraud Toolkit

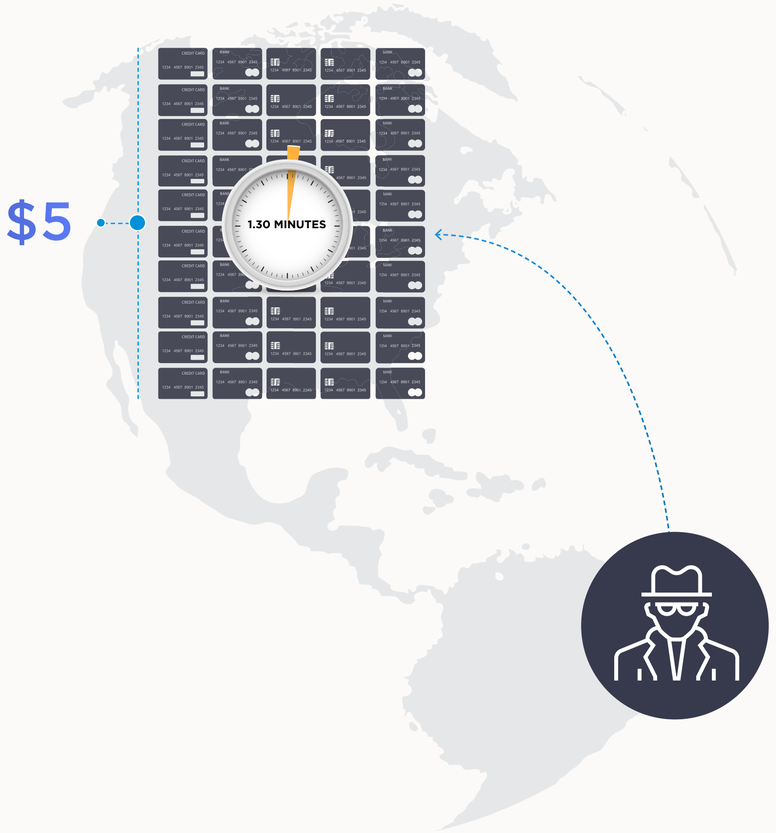
Leveraging ThreatMetrix digital identity intelligence, high-risk behavior was accurately identified in real time, alerting these Vantiv nonprofit customers to potential fraud and supporting a frictionless payment process.

The Result

- Accurately authenticated new and returning donors, improving their overall online and donor experience
- Identified and blocked fraudsters testing identity/ payment credentials
- Saved millions in reduced chargebacks and fees

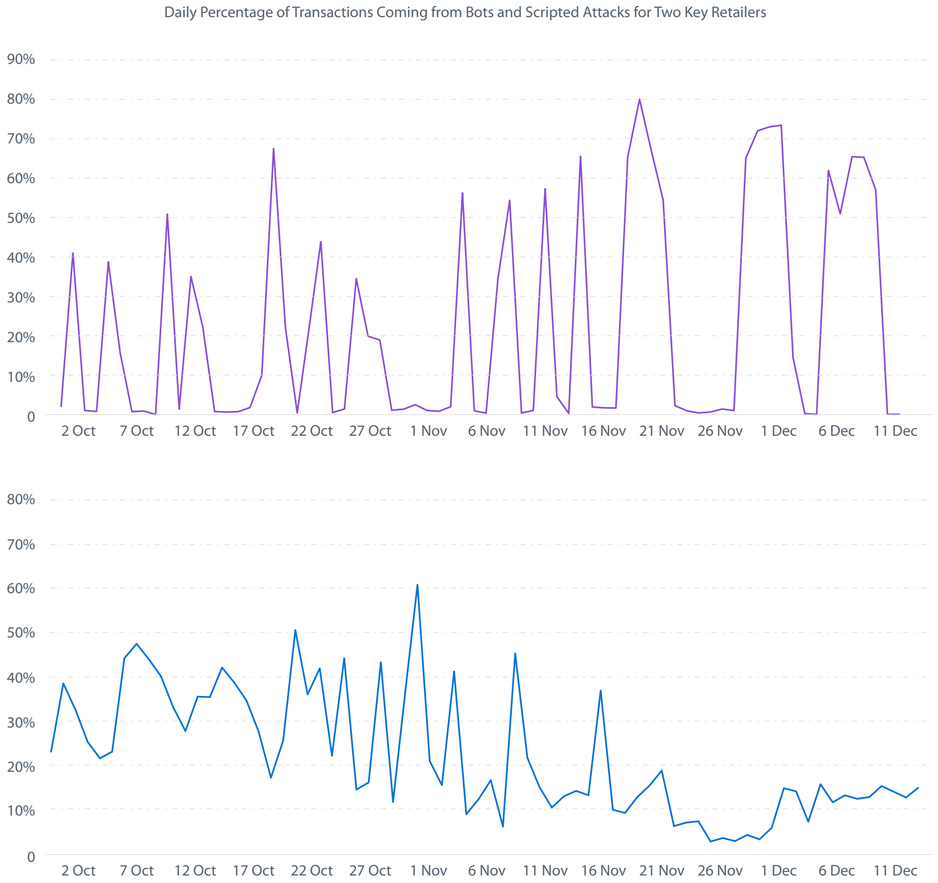
vantiv®

A fraudster based in Brazil using same device trying to make $5 payments with 50 different credit cards, within a minute and half, using a proxy in the US in November.



Besides from the US, we saw this kind of fraud mainly originating from Brazil, Egypt, Ghana, Jordan, Nigeria and Macedonia this quarter.

Threat Detection – A Constantly Evolving Cat and Mouse Game



Cybercriminals are using bots (a software application that runs automated tasks) to increase the efficiency of attacks on confidential data such as login and payment details. Customer experience is further compromised as botnets (networked / connected bots) run massive identity testing sessions to try and penetrate fraud defenses. Infected computers may not even realize they are part of these huge criminal networks.

The Network has seen a complex evolution of bot attacks during 2016, from basic bots, that are just used to perform velocity-based functions, to complex bots that are used in more advanced ways to spoof IP addresses, emulate browsers or spoof apps, to masquerading bots, that are attempting to mask their true context and pretend to be legitimate user traffic.

These various types of bots are used successfully in account validation attacks in order to try and monetize stolen identity data.

Leading online retailers were attacked relentlessly by bots, botnets and other scripted attacks. While millions of bot attacks were again detected this quarter for eCommerce merchants, overall bot numbers have declined this quarter, perhaps due to some of the high-profile successes in shutting down organized networks such as the Avalance botnet.

Despite this, however, bot traffic has at times made up around 90% of a key retailer's daily traffic, with sustain peaks throughout the period, making their impact widespread and at times, crippling.

ThreatMetrix uses context-based information to perform behavioral analysis of users to differentiate between a human and a bot the moment they land on the site.

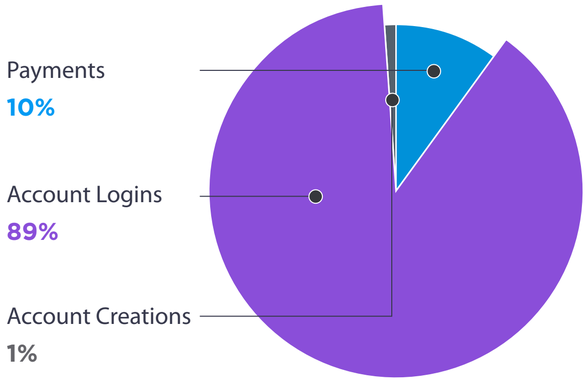
Financial Services Transactions and Attacks

Financial services transaction growth continues to be driven by mobile as users log in as often as daily to check balances on the go. Banks are embracing this pace of change, with many offering full service provision on mobile apps, facilitating a new generation of banking customers who are mobile only, and rarely, if ever, visit a branch.

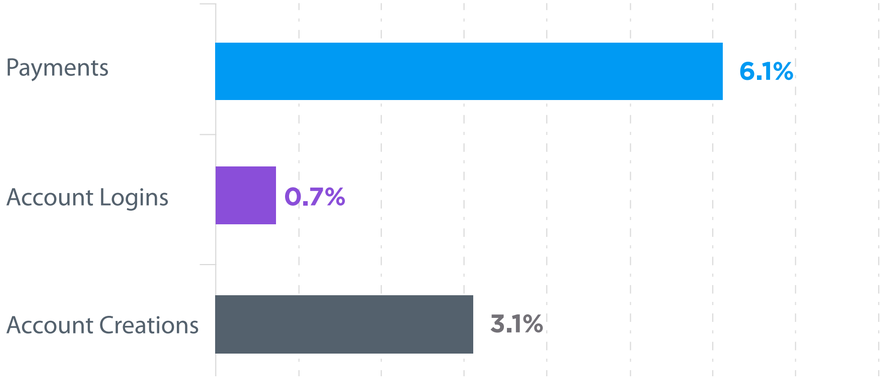
This contributes to the overall low reject rates on login transactions: the regular transactions help keep recognition rates of trusted users high. However, financial services organizations are less likely to block suspicious transactions outright, subjecting them instead to further review. Hence, the rejected transactions shown don't include access attempts that typically result in challenging a user to provide additional information.

The percentage of rejected payment transactions in financial services has grown 260% year-on-year, highlighting the increased risk from new and emerging FinTech platforms which are being increasingly targeted by fraudsters looking to make a quick buck on a P2P loan or fraudulent remittance.

Volume per Transaction Type



Reject Rate per Transaction Type



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.

Mobile Banking Drives High Customer Engagement

Almost 55% of financial services transactions are mobile with a 250% growth in mobile transaction volume year-on-year.

In addition, over 40% of users being mobile only. Mobile has higher user engagement with nearly twice as many mobile logins as desktop per customer.

As with previous years, an increase in the eCommerce activity during the holiday period also resulted in an increase in financial services transactions as users accessed their online banking accounts regularly to check balances and pay bills. Consumer logins for mobile banking increased on average 20% during the peak shopping days.

Q4 2016 represented the strongest mobile quarter for ThreatMetrix with a billion transactions in financial services alone.

Times per week customers log in to their bank account

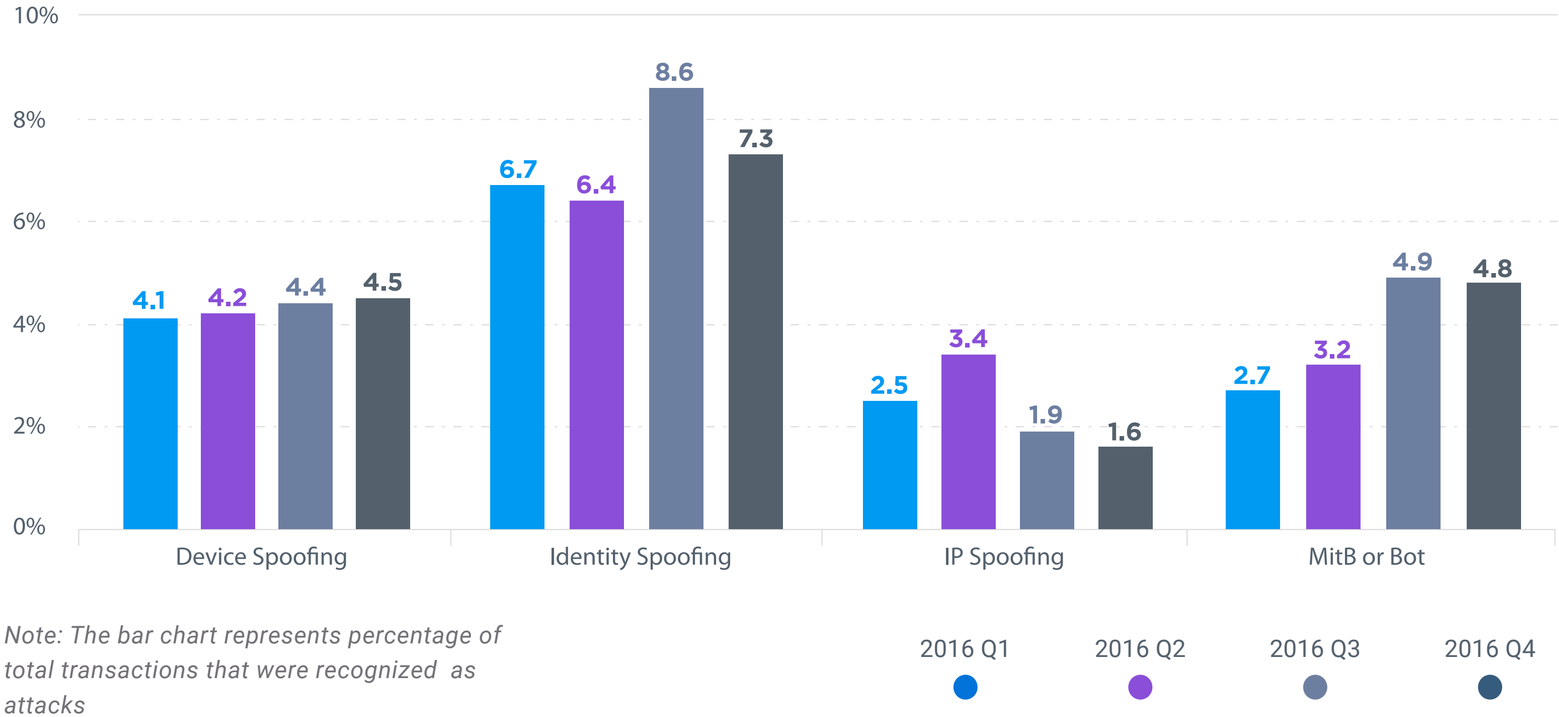
FinTech Attack Vectors

FinTech companies are being increasingly targeted by cybercriminals looking to capitalize on alternative lending and payment models, exploiting gaps and loopholes in what are predominantly digital systems, designed for superfast processing and agile product innovation.

The Network is typically seeing higher rejected transaction rates for FinTech than for traditional financial services institutions. This is set within the context of a big growth in digital wallet transactions this quarter as consumers relied on friction-free payment methods during the holiday season.

Loan stacking and bustout scenarios are common attack vectors, where fraudsters capitalize on time delays inherent in reporting loan agreements to credit bureaus. Stolen identity credentials and device spoofing techniques allow cybercriminals to bypass even complex application procedures.

At the same time fraudsters are using bots to mass test identity credentials and infiltrate trusted user accounts.



Note: The bar chart represents percentage of total transactions that were recognized as attacks

E-lenders Deep Dive

Online lending has grown in recent years and has driven financial inclusion for unbanked and underbanked customers, through an increased reliance on dynamic data for risk decisioning.

These e-lenders are seeing a surge in account creation transactions as digital users capitalize on the product innovation of new platforms, often offering new and niche services to a previously underrepresented population.

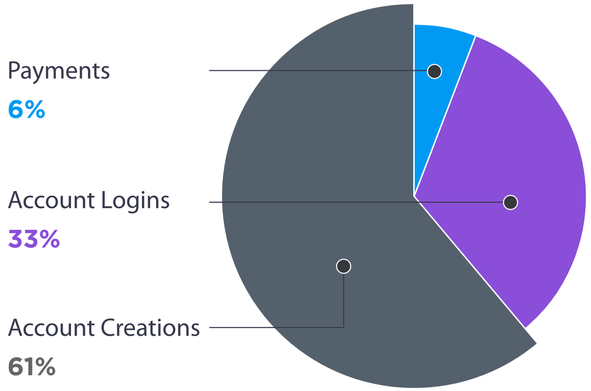
At the same time, the business of online lending is evolving, with rising interest rates and increased competition from traditional banks, creating pressure on profitability.

This is set within the context of growing attack levels: new loan application fraud is higher this quarter than ever before as cybercriminals buy, trade, augment and monetize stolen identity credentials for financial gain, perhaps seeing these new players as a softer target than some of the larger established banks.

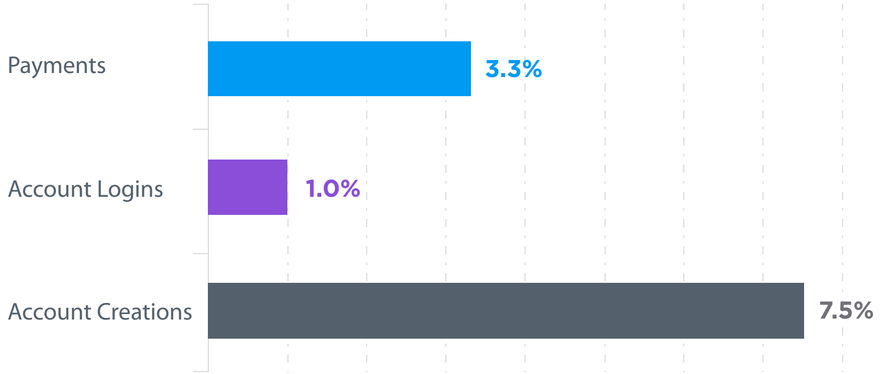
The challenge for e-lenders is that these profiles are becoming increasingly indistinguishable from authentic identities because they are created using a plethora of stolen data, making them a near blueprint of the real thing.

Peel beneath the layers, however, and you might reveal a spoofed device, cloaked location or anomalous personal credentials that can point to the Machiavellian character beneath. Digital identity data therefore becomes the critical differentiator to distinguish between fraudsters and genuine customers.

Volume per Transaction Type



Reject Rate per Transaction Type



P2P, Holiday Giving

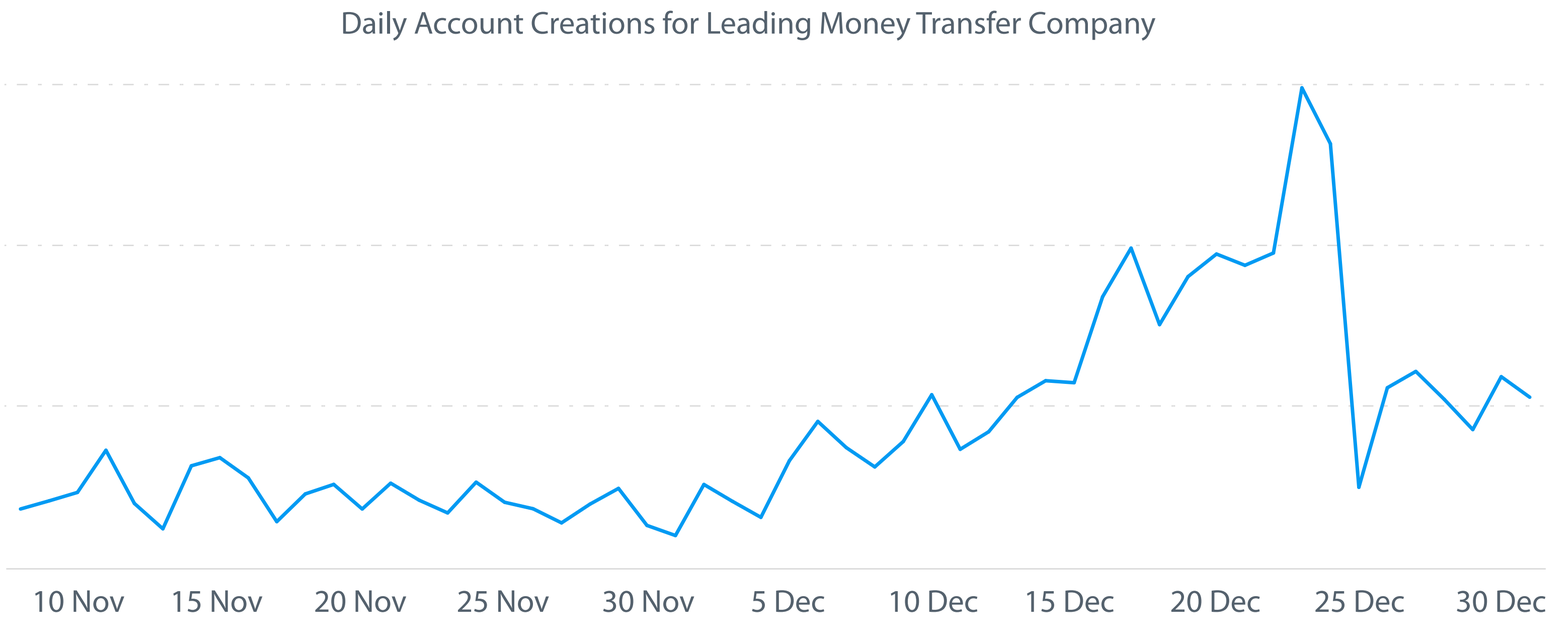
In a connected world, every year people send billions of dollars to friends and family across the globe.

Both established financial institutions and emerging providers are building solutions for digital consumers, enabling them to send money securely and instantly.

Money transfer operators across the globe are being targeted by fraudsters that have access to unsuspecting users' stolen credentials.

With the arrival of the holiday season, remittance volume goes up as users send money to their loved ones. Transaction volumes in The Network increased sharply until Christmas Eve.

Fraudsters target this increased activity by taking over legitimate accounts or opening new accounts to launder money through from previously hijacked bank accounts.

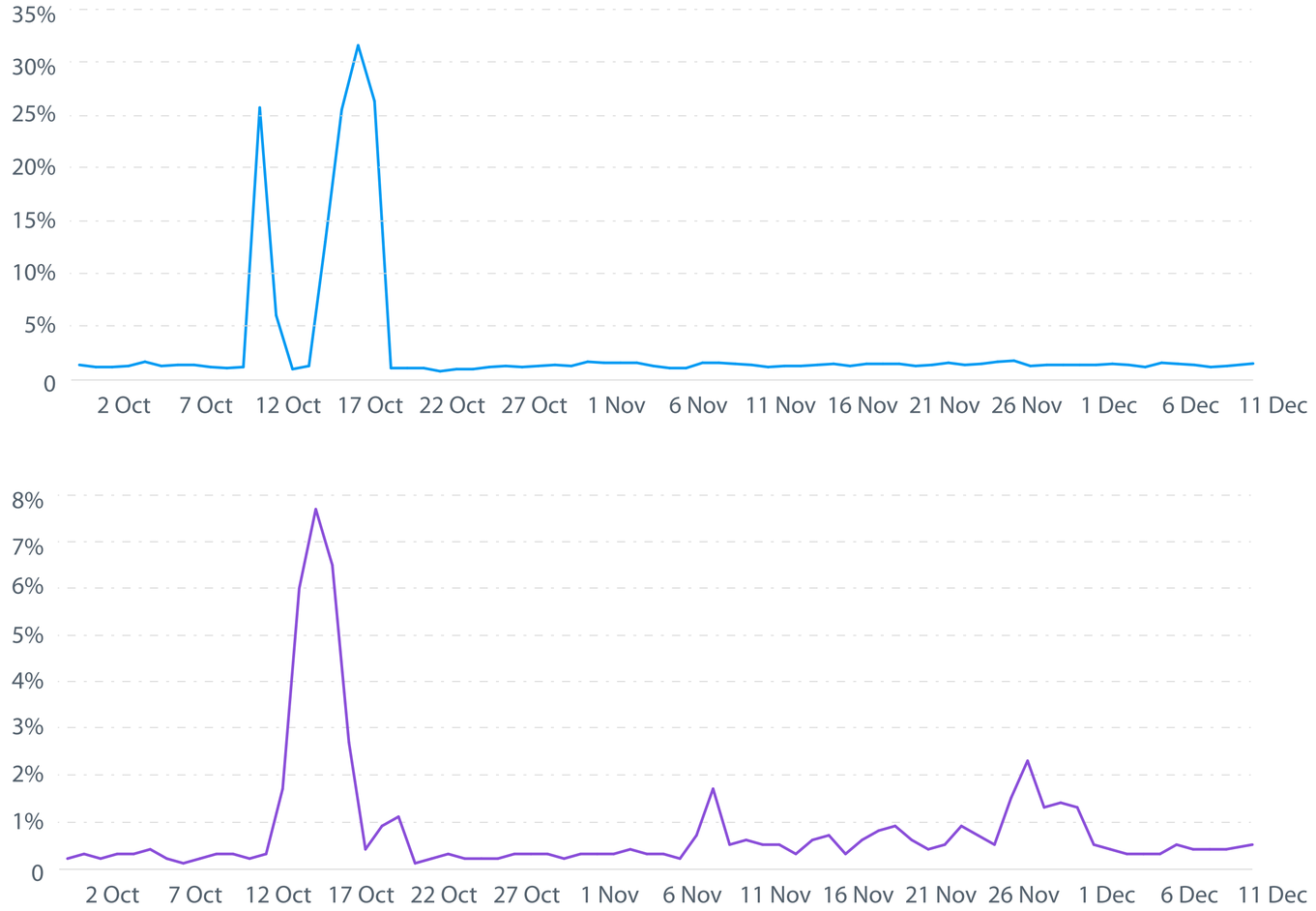


Evolving Bot attacks Target Financial Transactions

Cybercrime is becoming increasingly automated, sophisticated and is scaling exponentially through well organized crime rings which can allow fraudsters without the technical skills to nevertheless deploy complex attacks.

Financial Institutions continue to be targeted heavily across consumer touch points. For some of the large institutions, these spikes represent millions of attacks targeting a single organization and make up a high percentage of daily transaction volume. A significant portion of these attacks target FinTech providers' new account application processes. ThreatMetrix detected millions of credential testing attempts using bots / scripts this quarter.

Daily Percentage of Transactions Coming from Bots and Scripted Attacks for Two Key Financial Institutions



CASE STUDY

One Call Insurance

The Problem

One Call Insurance was being exposed to organized fraud rings and ghost brokers trying to register for fraudulent insurance policies.

One Call Insurance sometimes couldn't detect this fraud until the second policy appeared, so the initial fraud was slipping under the radar.

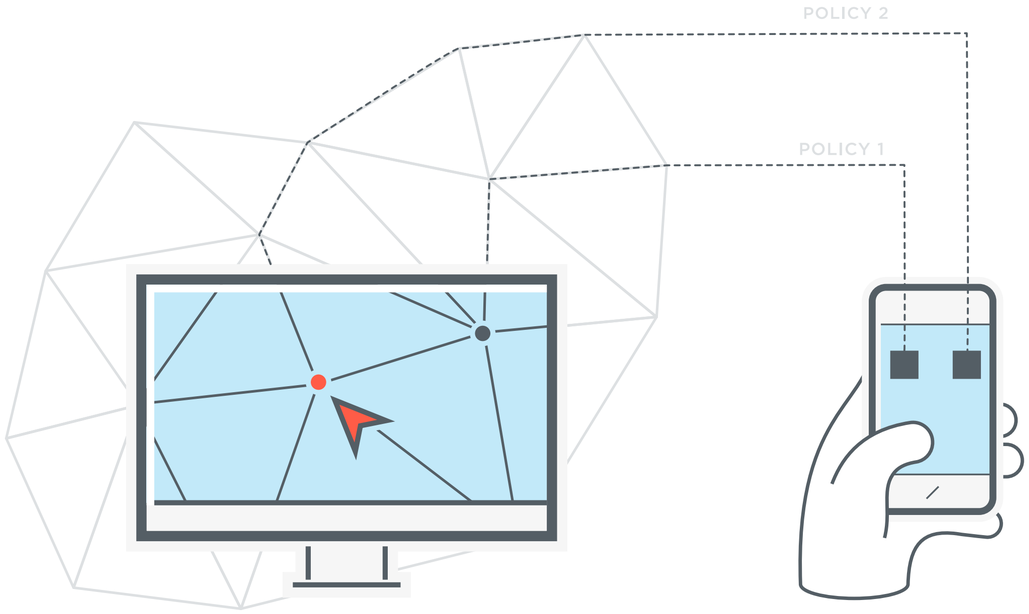
The Solution

One Call Insurance augmented device data with Digital Identity Intelligence from ThreatMetrix so it could build a more accurate risk profile of every policy application, even if it hadn't seen the device before.

The Result

- ThreatMetrix rules predicted fraud up to a 50% likelihood, a significant increase compared to the previous device-based solution.
- 60% increase in fraud detection rate.

One Call INSURANCE



Media Transactions and Attacks

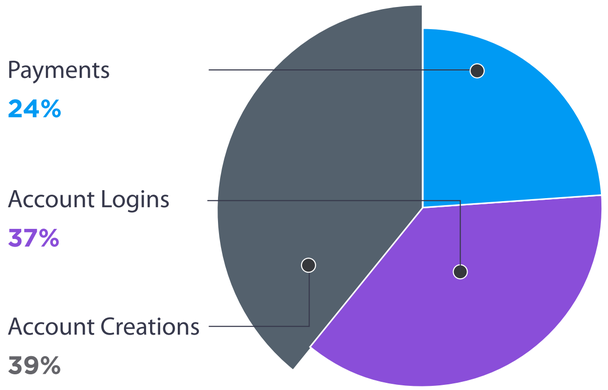
ThreatMetrix detected and stopped over 25 million attacks this quarter, representing a ~60% year-on-year growth in attacks. These attacks included account creation fraud, bogus reviews and listings, account takeover and payment fraud.

Fraudulent new account registrations continue to grow, and have increased nearly 300% over the previous year as fraudsters used the relatively modest sign up requirements of media organizations as a breeding ground to test stolen identity credentials.

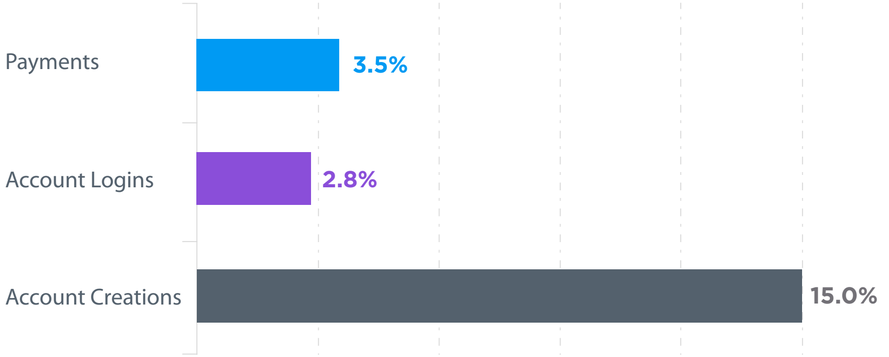
Travel review sites, holiday marketplaces and social media organizations rely heavily on a currency of trust between members and users; cybercrime activity can seriously jeopardize the reputation and integrity of media platforms. Media threats are therefore beginning to take a new form: fraudulent reviews, fake news and phony listings are the attacks of the future and are becoming the key way to perpetrate fraud and monetize stolen credentials.

Despite the fact that consumers primarily use their mobile devices to access social media, consumer content or read user reviews, desktop is still the most convenient way to write reviews. Desktops are therefore increasingly being used by fraudsters to create mass scale fraudulent reviews and listings, as well as to spam malicious content.

Volume per Transaction Type



Reject Rate per Transaction Type



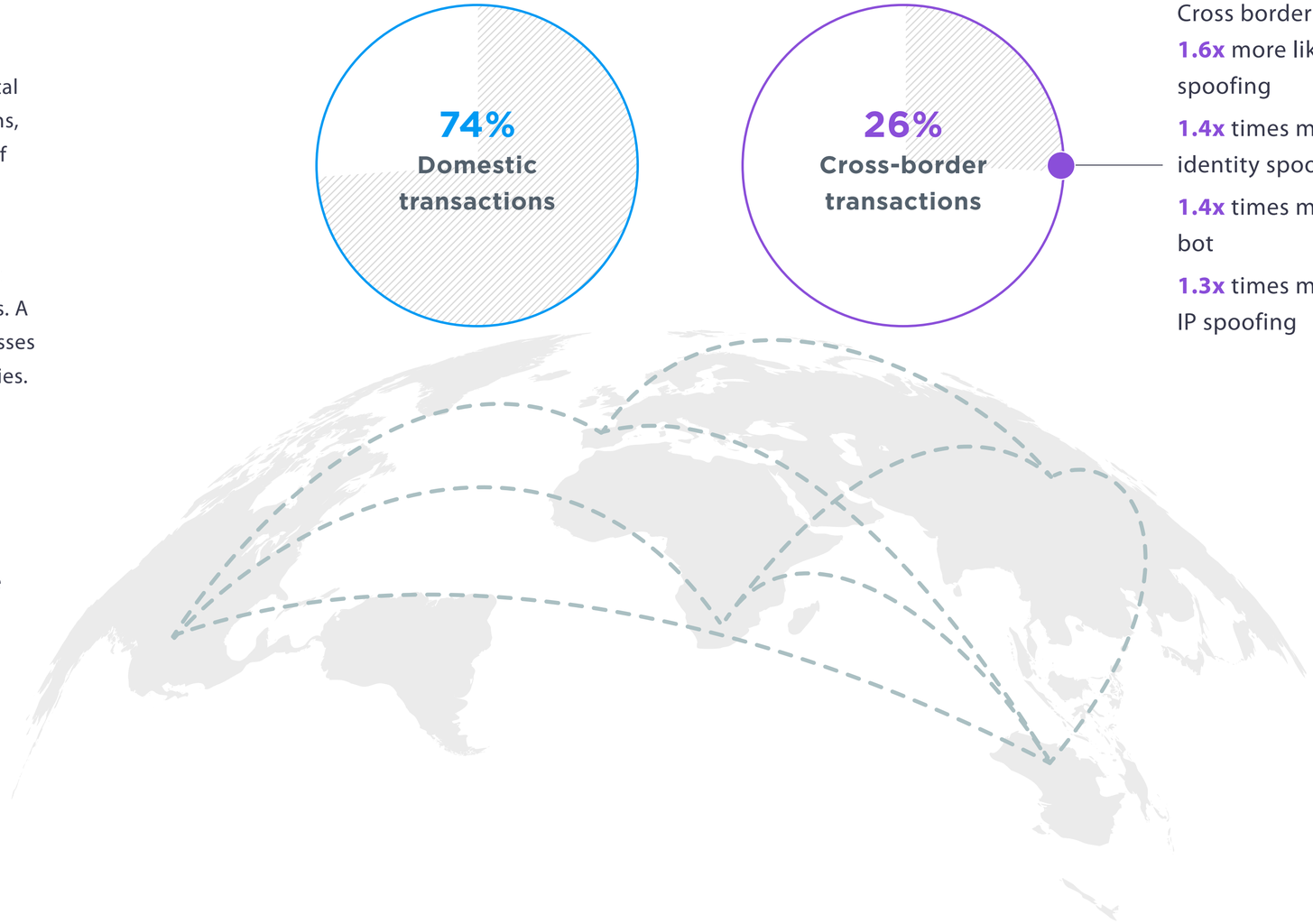
The Continued Rise of Global Transactions

A quarter of transactions in The ThreatMetrix Digital Identity Network are now cross-border transactions, highlighting the ever-increasing digital mobility of global connected users.

However businesses continue to approach cross-border transactions with caution; hence the reject rate is 2.3 times higher than domestic transactions. A big driver of this is the custom rules set by businesses that often reject transactions from specific countries.

Cross-border traffic is also more susceptible to identity spoofing and bot attacks than domestic traffic, as cybercrime continues to be a global and well-organized criminal network

As cross-border transactions continue to be a core feature of Network traffic, businesses must adopt a more global, dynamic approach to verifying transactions.

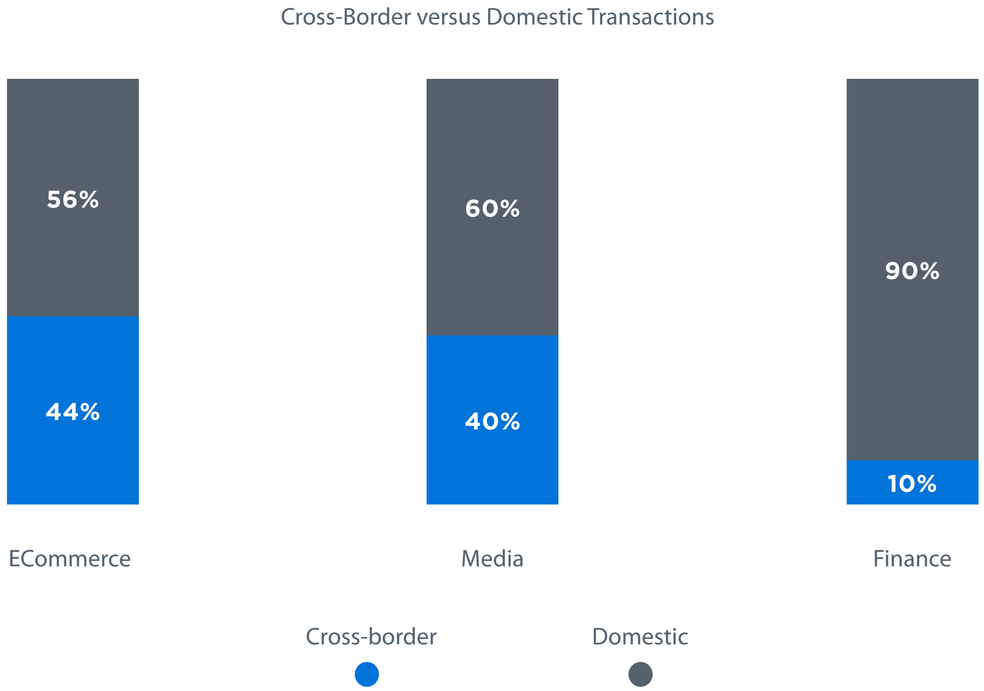


Cross-border by Industry

Media and eCommerce traffic is increasingly coming from a global, migrating population, as users are less and less confined to country / regional boundaries.

While these transactions are still considered risky, businesses are recognizing the potential of a global consumer base and are working hard to lower their rejection rates, using more than just static legacy rules to accept or reject transactions.

However, banking and finance still remains a primarily domestic activity and as expected financial services has a relatively low instance of cross-border traffic. It is also treated with extreme caution, rejected at 5 times the rate of domestic transactions.



Top Attack Vector Trends

ThreatMetrix identified 122 million fraud attempts during this period. This represents a 35% growth over the previous year.

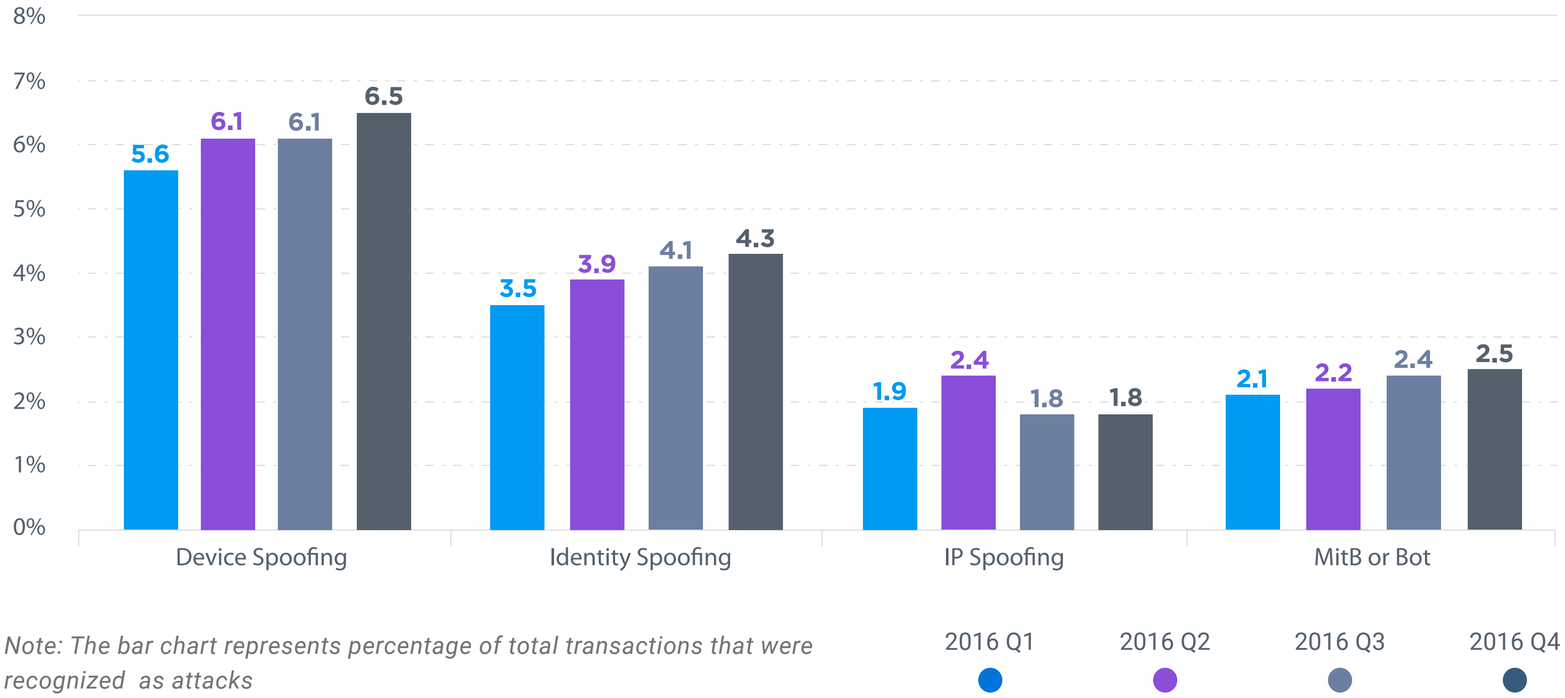
Attack vectors are analyzed in real time by ThreatMetrix global policies. However, some attacks use multiple vectors, making them more complex and harder to detect.

Key attack vectors are growing, driven by availability of more sophisticated device spoofing tools combined with hacked and breached identities.

New account creations are especially vulnerable: fraudsters use stolen identities along with malware, phishing or bot attacks to defraud businesses.

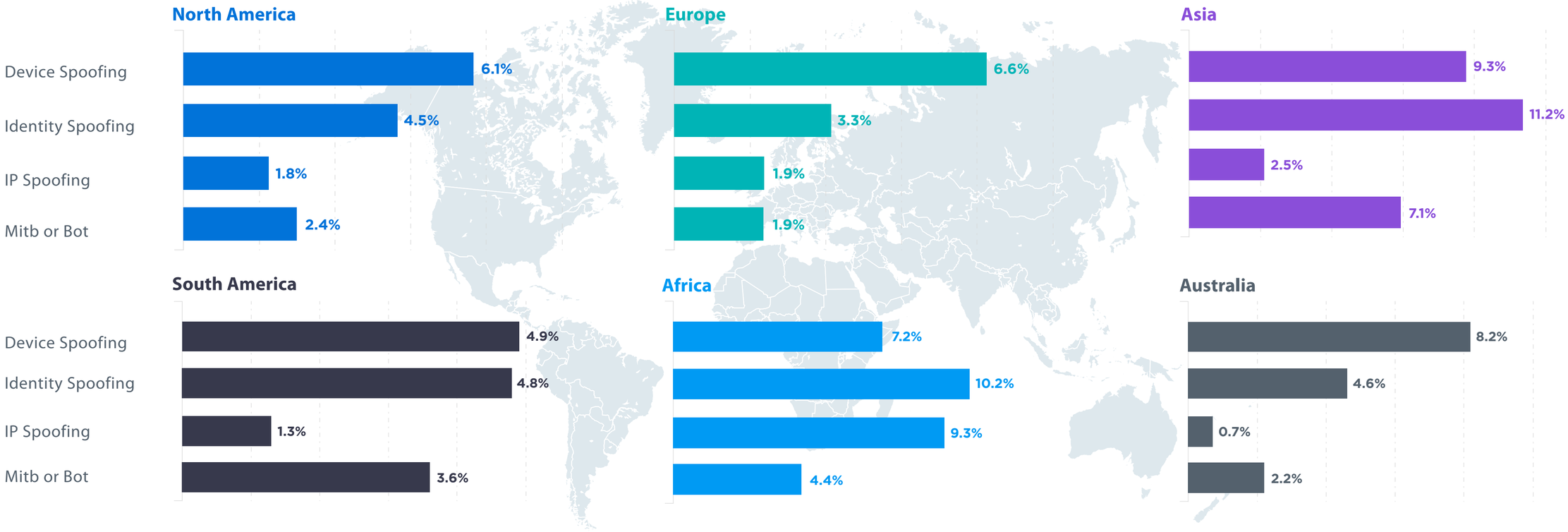
Malware, Man-in-the-Browser (MitB) and bots are the most malevolent attacks. Their ability to quietly compromise nearly any online authentication system, (including two-factor authentication), means these attacks are normally reserved for operations with large payouts.

ThreatMetrix counters this growth in identity-based attacks using key intelligence from the ThreatMetrix Digital Identity Network, combined with behavioral analytics, to accurately distinguish fraudsters from legitimate users.



Note: The bar chart represents percentage of total transactions that were recognized as attacks

Attack Vectors by Continent

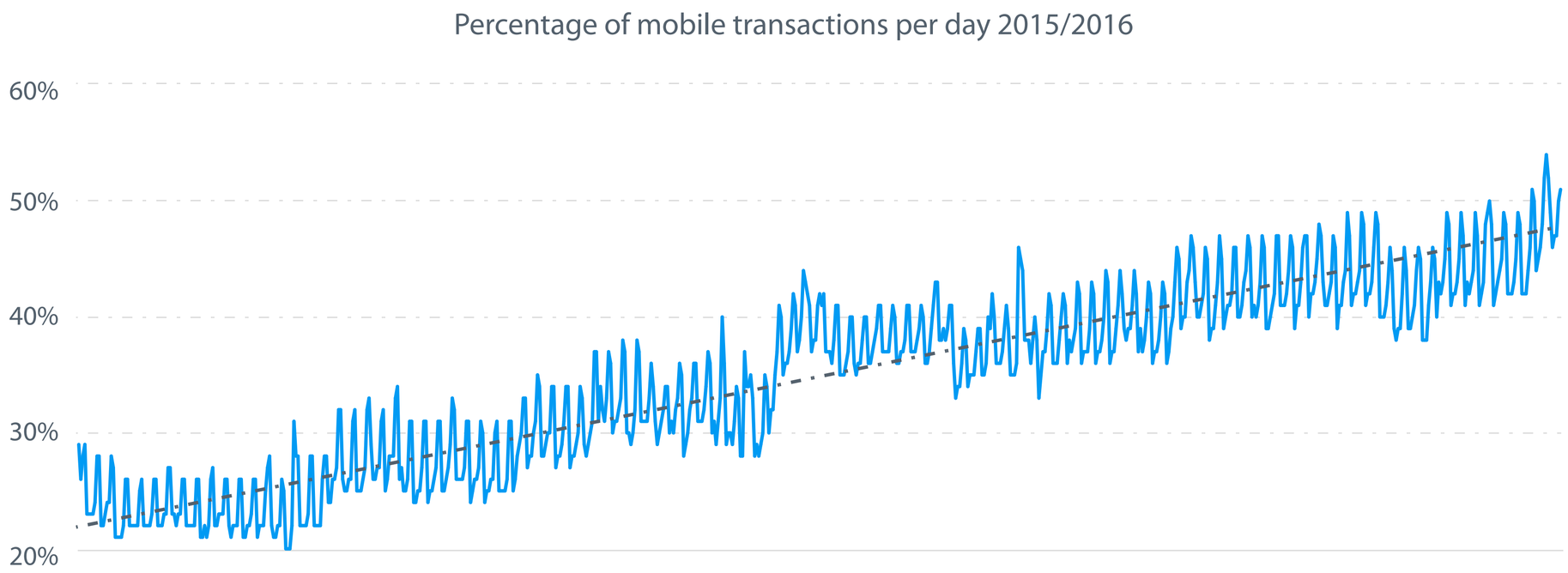


With 6 billion user identities compromised since 2013 – including 2 billion alone in 2016 - spoofing or impersonation attacks are growing across the globe.

Identity spoofing is the leading attack vector in emerging economies, as well as for industries that target unbanked and underbanked populations, as organized identity verification tools are not as prevalent for these users.

Global businesses need the ability to incorporate regional variances and gaps in identity verification services without impacting the online experience for true digital customers.

Growth of Mobile Transactions



Mobile transactions grew 130% year-on-year, primarily driven by the increase in financial services account logins as users embraced the ease and convenience of mobile banking apps.

Over 50% of account creations now come from mobile, rising to 54% for media account creations.

The ever-increasing popularity of mobile apps encourages a high proportion of returning customers in comparison to mobile browsing.

Although mobile transactions are still safer than desktop, attack vectors have evolved in 2016 to incorporate mobile bots, illustrating the advanced tactics of cybercriminals looking to capitalize on the growth of mobile commerce.

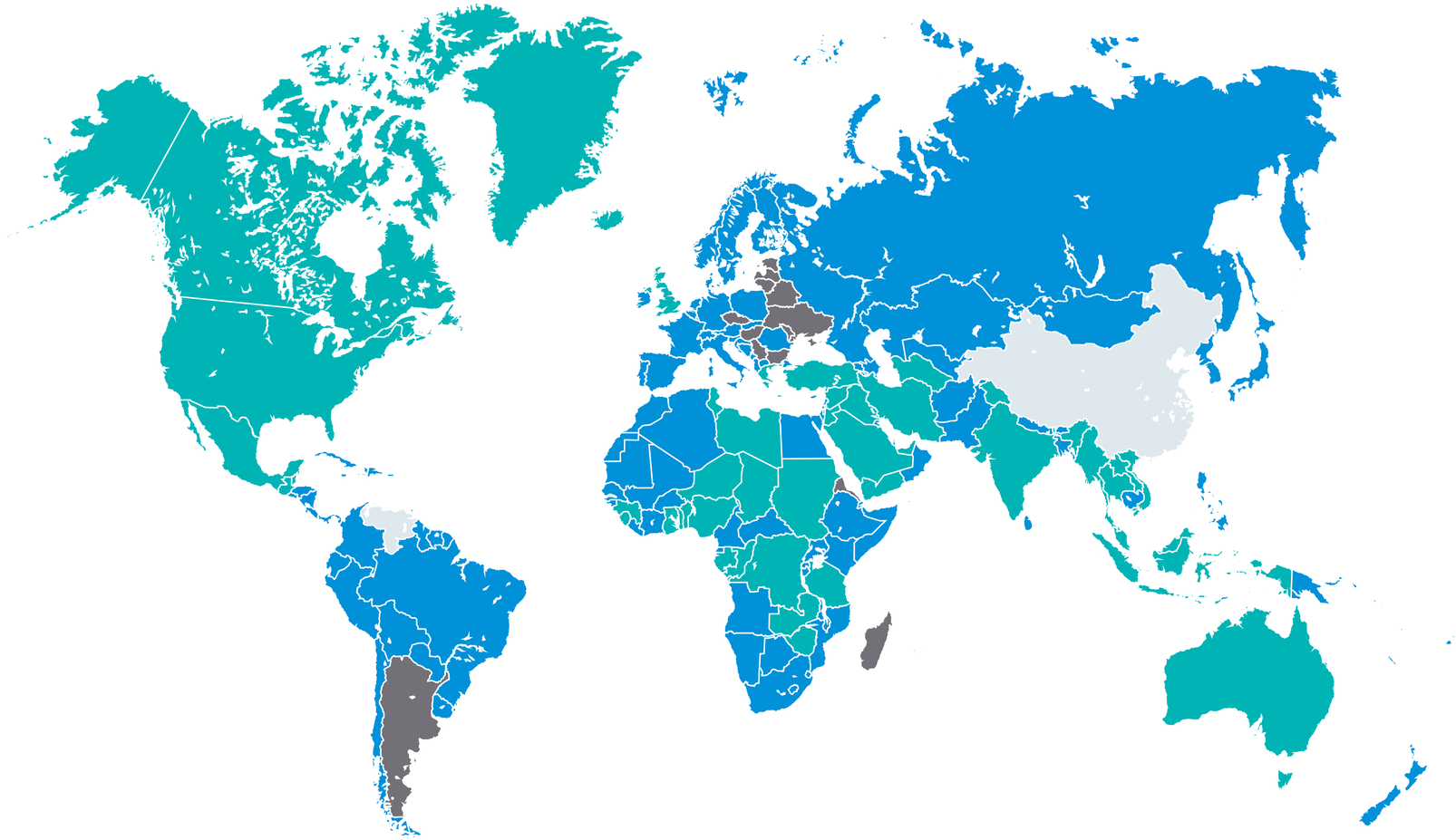
Mobile Transaction Prevalence

The network analyzes mobile transactions from over 200 countries and territories across the globe.

With each quarter, mobile transactions are growing across developed and emerging economies. Mobile-only users are also growing.

Mobile Transactions per Country

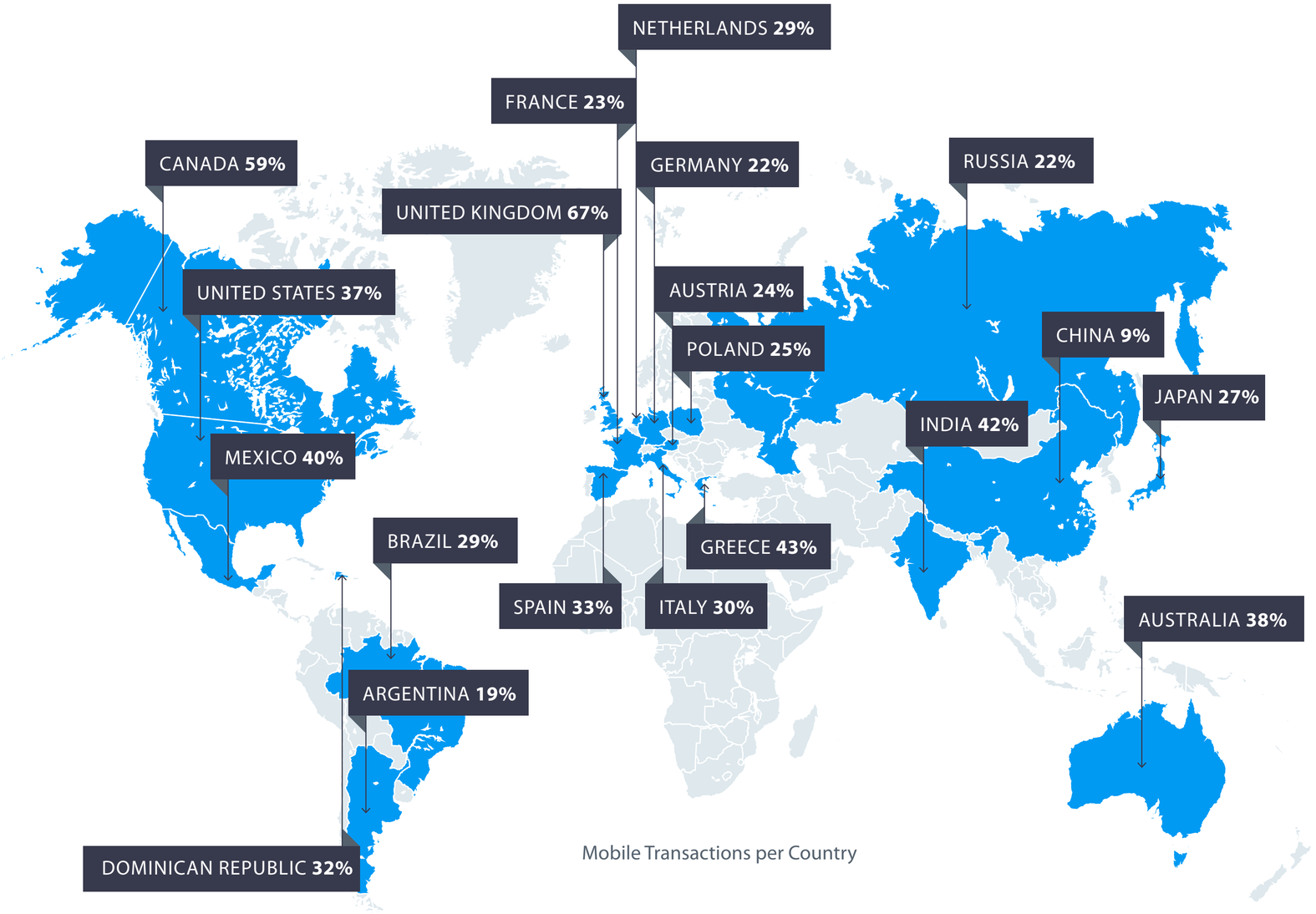
- > 35%
- 20 - 35%
- 15 - 20%
- <15%



Top Digital Nations

In 2016, mobile penetration increased significantly in several key Central and South American countries including Mexico, Dominican Republic, Brazil and Argentina.

This trend was also seen in some emerging European economies such as Poland and Greece.



Mobile Transactions per Country

Mobile Versus Desktop Transactions and Attacks

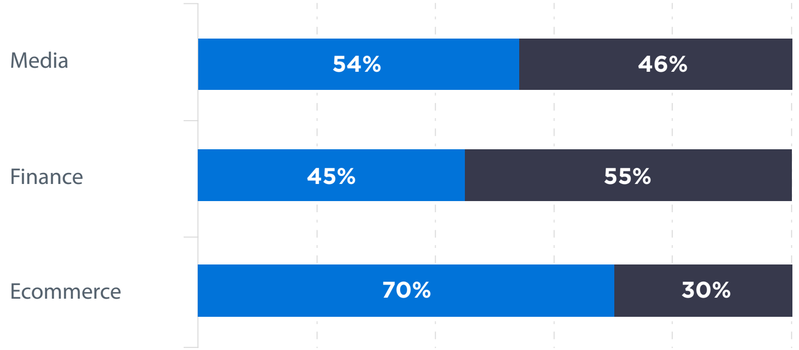
Mobile-based commerce represented 45% of the total transactions analyzed by The Network in Q4.

Mobile has become the primary way for users to browse and access their accounts as well as sign up for new services. The biggest driver of this growth is coming from financial institutions whose share of mobile has steadily grown. This is driven by user adoption as well as deployment of digital solutions by the banks.

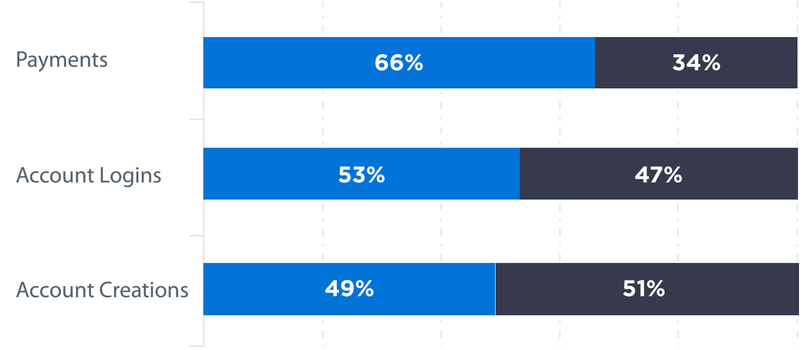
Payments are still primarily desktop-based, driven by users' preference for the convenience of a larger keypad. However, this will evolve over time as more global users adopt digital wallets and move towards one touch payments.

The prevalence of stolen identities and tools to enable cloaking / spoofing is causing attacks targeted at mobile devices to evolve and increase. Fraudsters are continually using unsecured wireless networks to intercept user credentials, encouraging users to download hacked versions of legitimate applications from third party stores, or looking for ways to intercept personal information that can be inadvertently leaked by legitimate mobile applications.

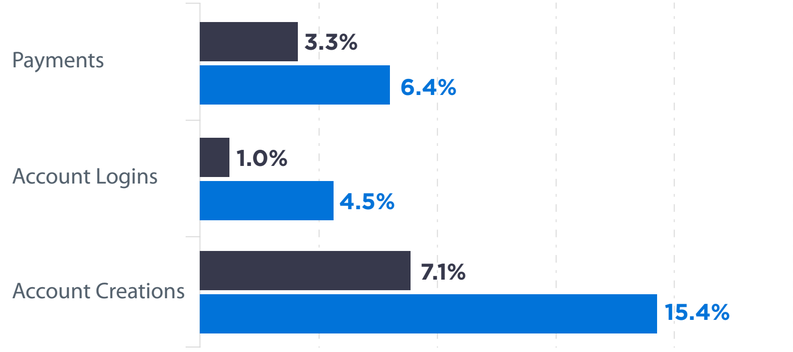
Volume Desktop vs Mobile per **Industry**



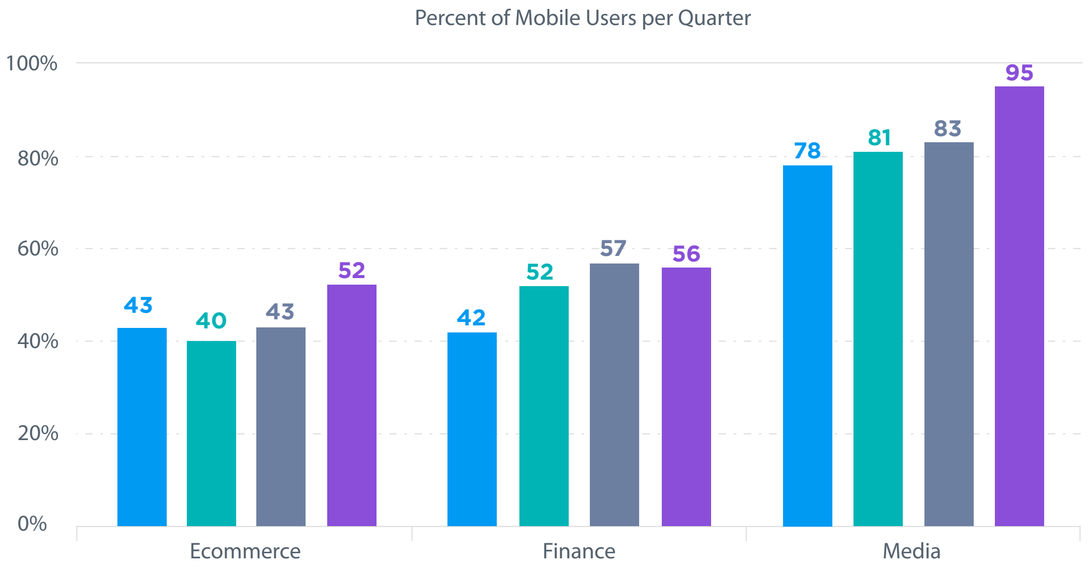
Volume Desktop vs Mobile per **Transaction Type**

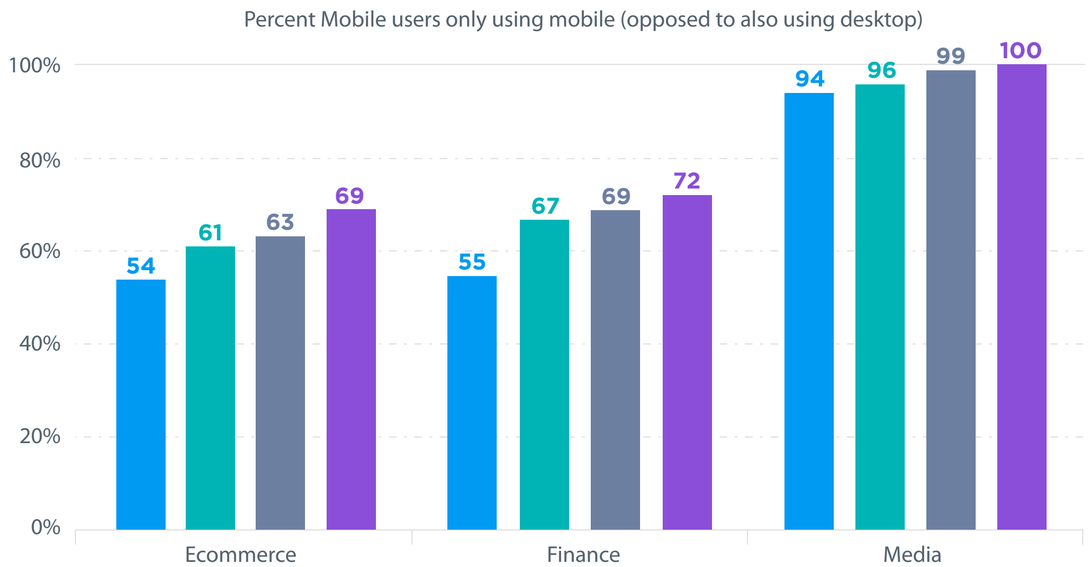


Reject Rate Desktop vs Mobile per **Transaction Type**



Cross-device Usage





Cross-device usage continues to grow: more users accessed their bank account, made payments, streamed content and signed up for new accounts using connected devices.

Mobile-only users are growing across all industries, with the strongest footprint in media, highlighting the fact that mobile app development strategies are paying off and some users are doing away with desktops entirely.

As consumers move seamlessly between screens on connected devices, they expect their experience to be consistent and frictionless. This requires a holistic recognition of trusted returning users that looks beyond just devices. Businesses need to evolve from a "mobile-first" approach to a "digital-first" approach.

Looking Ahead

2017

Rise of the Global Mobile Customer: Static users transacting on a stationary device is a thing of the past. In 2017, mobile transactions will outpace web transactions across the board, with cross-border traffic continuing to rise.

Consumer Experience Becomes Critical: Brand loyalty will depend on how consumers are treated across locations, channels, and devices.

The 'Cybercrime Franchise-in-a-Box': 2017 will bring increased availability of tools that will allow criminals without technical skills to carry out sophisticated attacks.

Rise of 'Identity Farms': New attacks will focus on gathering more information to beef up stolen identities, rather than immediate monetization.

Ineffectiveness of Static Identity Data: In light of rampant data breaches, static data elements cannot be trusted. Dynamic information around one's digital identity will be crucial to differentiate good customers from bad.

Analytics Make All the Difference: Organizations must align authentication and identity verification with a multifarious user base. Organizations will increasingly rely on dynamic behavioral analytics to identify high-risk behavior on an individual user level.

Trust Becomes the World's Most Valuable Currency: Companies need to deploy new digital identity solutions that establish the trust level of each user across all data, devices, locations, and behavior—cross-referenced in real time against worldwide threat intelligence.

What the latest crop of data breaches has brought into even sharper focus is that isolated pieces of information that tie a user to an account – whether these are usernames, passwords, security questions or personal information – are not the authentication methods of the future. In fact, any static information that is capable of being stored by a company is also open to being breached, and is therefore an outdated way of thinking about secure authentication, identity verification and fraud prevention.

It is becoming increasingly clear that the only true way to keep the online digital world safe and secure, (and processing transactions in the manner that technology savvy consumers expect), is by analyzing the digital identity of every online user, an identity that is built on dynamic, shared intelligence harnessed from sources far wider than the individual companies a user transacts with. In addition, this should be underpinned by the following two pieces of intelligence:

Behavioral analytics: Analysis of a user's intricate and often diverse online footprint can give us a unique way of identifying anomalous and high-risk behavior

Machine learning: This can provide a predictive model based on past behavior and transaction data, ideally using a clear-box approach to produce a more accurate and actionable model.

It is only by using this holistic, crowdsourced approach to digital identities that companies can be more confident of accurately differentiating fraudsters from genuine customers. In the case of Yahoo, the cookies might have been forged, but the online footprint of those fraudsters would have been markedly different to the genuine users, and it is up to Yahoo to be able to detect that in order to protect sensitive customer data.

The ThreatMetrix Digital Identity Network is the largest repository of digital identities in the world and analyzes billions of transactions every year, preventing tens of millions of attacks. It's a compelling solution to an ever-growing problem.

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. 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 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. 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 (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.

Industry Types

Financial Services: includes mobile banking, online banking, online money transfer, lending, brokerage, alternative payments and credit card issuance.

FinTech: includes companies that use technology to make financial services more efficient with a purpose of disrupting incumbent financial systems and corporations that rely less on software.

ECommerce: includes retail, airlines, travel, marketplaces, ticketing and digital goods businesses.

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

Common Attacks

Account Creation 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 creation, account login and payments) from mobile devices and computers received and processed by the ThreatMetrix 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.

San Jose (Corporate Headquarters)

160 W Santa Clara St, Suite 1400
San Jose, CA 95113
Telephone: +1 408 200 5755
Fax: +1 408 200 5799

London

201 Borough High Street
London, SE1 1JA, United Kingdom
Telephone: +44 (0) 20 3239 2601

Paris

13 Rue Camille Desmoulins
92130 Issy-les-Moulineaux
France
Telephone: +33 (0) 1 58 04 24 03

New York

5 Penn Plaza, 23rd Floor
New York, NY 10001
Telephone: +1 212 896 3987

Sydney

Suite 1202, Level 12, Tower B
799 Pacific Highway
Chatswood NSW 2067
Australia
Telephone: +61 2 9411 4499

Amsterdam

The Base, Tower C
Evert van de Beekstraat 1
1118 CL Schiphol
The Netherlands
Telephone: +31 (0) 20 800 0637

Japan

Otemachi Bldg. 4F FINOLAB
1-6-1 Otemachi, Chiyoda-ku,
Tokyo 100-0004 Japan
Phone: +81-(0)3-4530-9576

Hong Kong

Telephone: +852 36 698 341

SALES

Telephone: +1 408 200 5700
Email: sales@threatmetrix.com

SUPPORT

Telephone: +1 408 200 5754 / +1 888 341 9377
Email: tmsupport@threatmetrix.com

PARTNERS

Email: partners@threatmetrix.com

PUBLIC RELATIONS

pr@threatmetrix.com

ThreatMetrix®