ThreatMetrix®

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

Americas: +1 408 200 5700
Asia Pacific +61 2 9411 4499
EMEA +31 (0)20 800 0638

sales@threatmetrix.com
partners@threatmetrix.com
threatmetrix.com

2015 Q4 CYBERCRIME REPORT

FOREWORD

There has been a lot of talk about the many high profile data breaches and their irreversible impact on the face of cybercrime. However, as we look back at 2015, the biggest theme that emerges is the continued digitization of consumers that is fuelling the growth of the "digital first" economy. The growth of online and mobile transactions continues to outpace brick-and-mortar commerce, epitomized by this year's holiday shopping which occurred predominantly online rather than in-store. As digital stores and channels gained sales and traffic at the expense of brick-and-mortar stores which lost traffic, the concept of lining up for deals on 'Black Friday' seems like another old business concept that needed "digital innovation".

Digital commerce is providing a launch platform for small or niche businesses that previously struggled to keep up with the established players. Internet-only banks, small lenders and niche insurance brokers can respond with more agility to meet the evolving needs of digital consumers including the unbanked and underbanked population, who previously had little access to traditional banking services. Meanwhile, by tapping in to the global reach of the internet, crowdfunding platforms are transforming money lending into a democratic and dispersed phenomenon, no longer the sole domain of the traditional bank. Banks that fail to embrace the opportunities of digital technology, such as automation, new product development and superior customer experience, could see significant erosion of net profits in the coming years.

Commerce has transformed from static, location-centric and in-person to mobile, fluid and anonymous and financial institutions and other businesses alike are evolving to maintain relevance. The unprecedented availability of customer data is prompting exciting innovations in new and existing industries. At the same time, security and fraud risks continue to grow at a rapid pace as fraudsters seek to capitalize on easily available identity data and the anonymity of online transacting. The relentless attack levels show that businesses need to work hard to protect their customers from the damage of cybercrime, which can have far-reaching consequences for their brand, reputation and revenue.

In this context, how can businesses be confident that they are transacting with trusted users? More importantly, how can they really verify identities without disrupting customer experience? After all, the very reason customers are adopting online services is because they are always on, allowing instant, user-driven access that works in tandem with their busy, diverse lifestyles. Companies must find a way to establish true user identity without impacting other customers. This is where understanding a user's true digital identity comes in. Most fraud and authentication systems have incomplete knowledge of a user's history of digital interactions across channels, devices and applications. Even if they do, so-called big data solutions still lack a single 'digital decision platform' capable of making real-time trade-offs between convenience and risk.

As we begin executing our business strategies for 2016, real-time decisions based on the digital DNA of customers combined with their unique online footprint and identity graph can knit together trusted digital identities that fraudsters can't fake. Leveraging the power of digital identities to establish trusted behavior unique to each user is the best way to rout out fraudsters, malware and bots without creating friction. As the evidence shows in this report, cybercrime is very real and growing and the businesses that will survive and thrive are those that move beyond just issuing free-credit reports and new credit cards, and invest in smarter authentication and fraud analytics that ultimately reduce the value of stolen credentials in the hands of cybercriminals.

Alisdair Faulkner

Chief Products Officer

2015 YEAR IN REVIEW

2015 HIGHLIGHTS

KEY TRENDS

Cybercrime continues to be a global, organized and well funded operation.

Strong mobile growth as more user interactions move to smartphones.

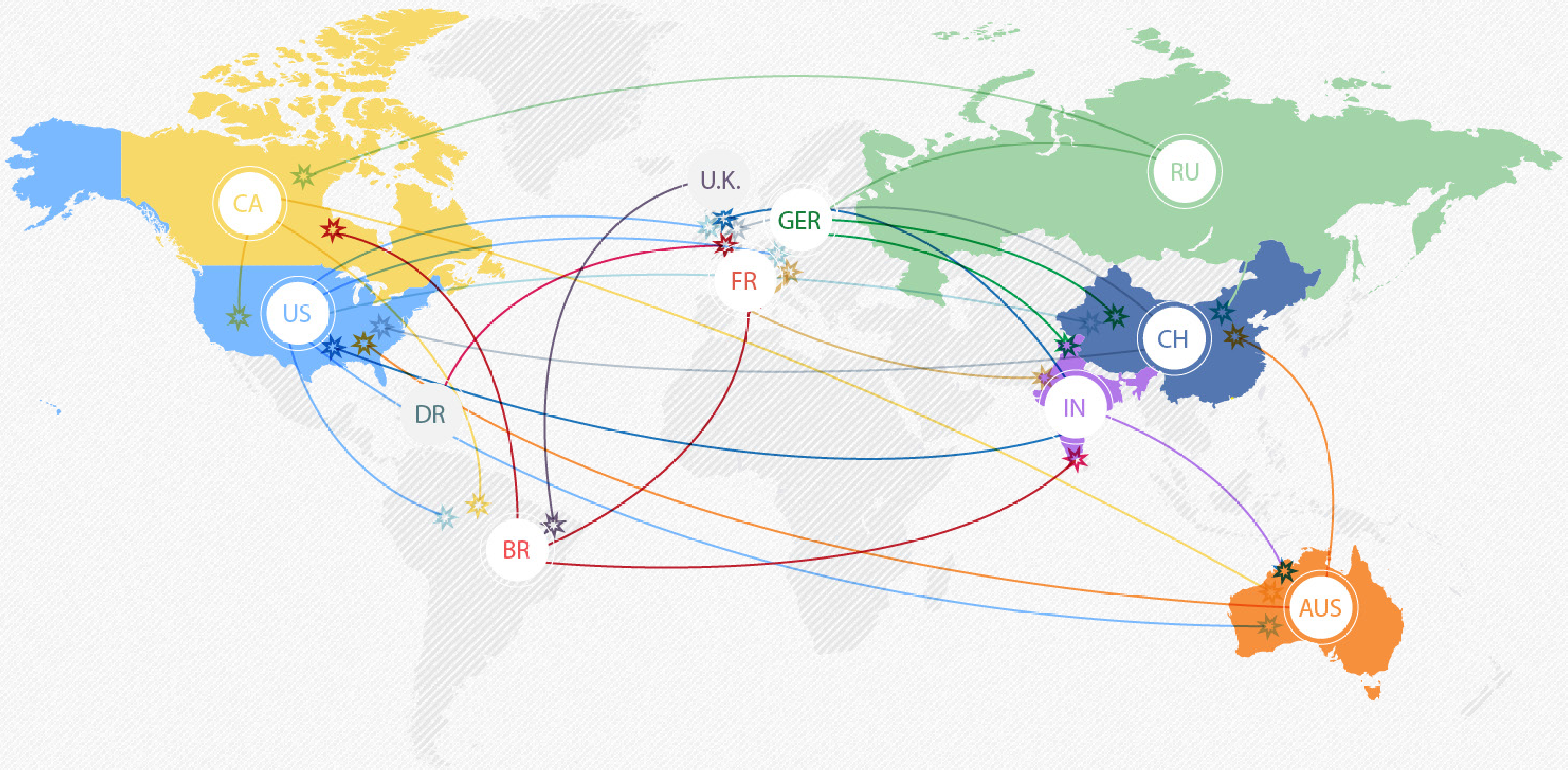
Holiday season shopping goes digital.

Attacks are increasing as bots, botnets and other crimewares take center stage.

Increase in account takeover and new account origination fraud, signaling the end of traditional identity assessment.

Real-time recognition of returning customers is critical in the fight against cybercrime.

ATTACKS ARE GLOBAL AND ORGANIZED



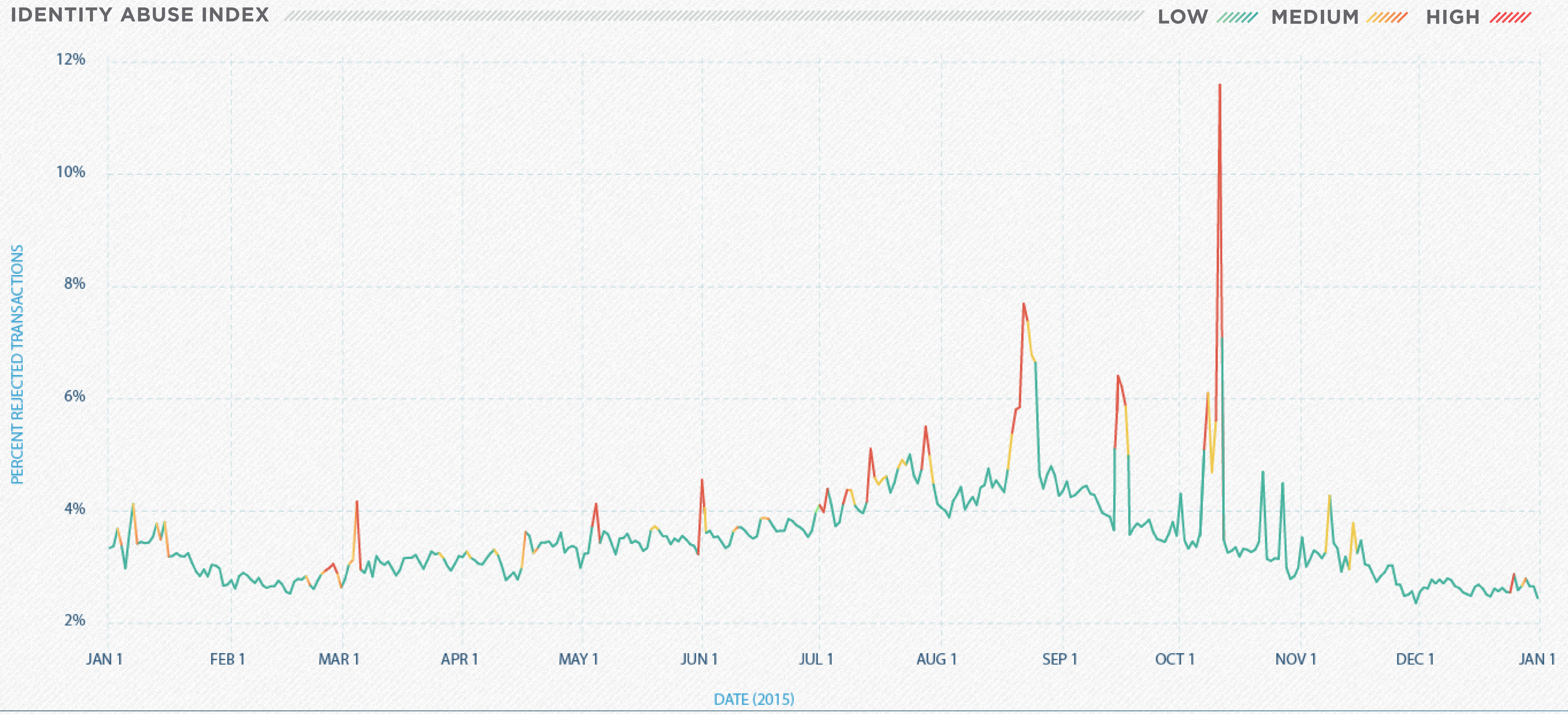
DATA BREACHES AND BOTS DRIVING CYBERCRIME SURGE

ThreatMetrix provides an indicator for cybercrime attacks using stolen identities and credentials through analyzing transactions from The Network.

- The key cybercrime peaks in 2015 were driven by the persistence of data breaches which flood the dark web with easily available stolen identity data, as well as specific organized bot / botnet attacks which launched large-scale identity testing sessions on logins of key large organizations.

Each transaction and attack trend is analyzed in the context of an identity (or more accurately an account) being abused and can provide insights into the threat environment now and in the future.

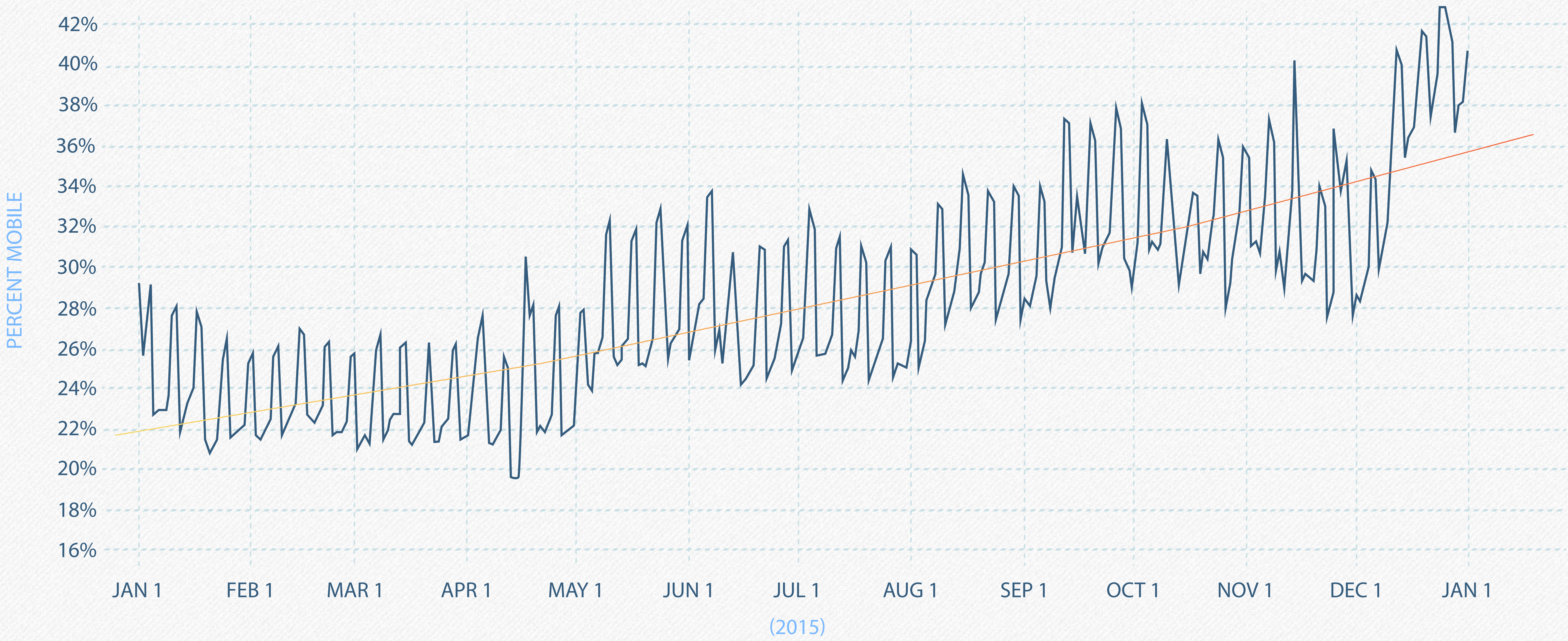
By using statistical models to identify deviations greater than the medium term average, the threat level was elevated 19% of the time in 2015.



MOBILE FIRST BUSINESSES

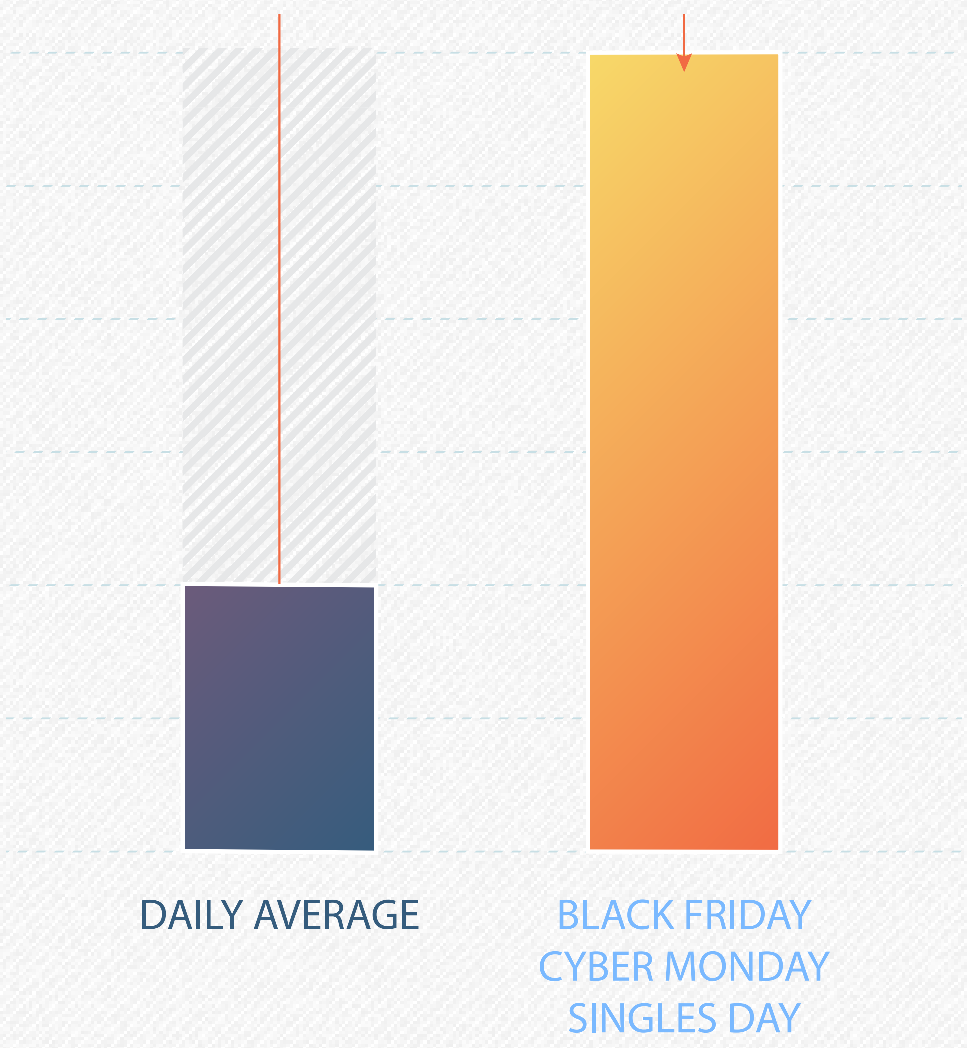
Mobile share of transactions continues to grow as more and more transactions are moving to smartphones. This is further fuelled by businesses deploying tools and apps to engage mobile consumers. However with the growth of mobile-based e-commerce and banking, online businesses are exposed to a new class of device and mobile app based attacks.

DAILY MOBILE TRANSACTIONS



HOLIDAY SHOPPING GOES DIGITAL

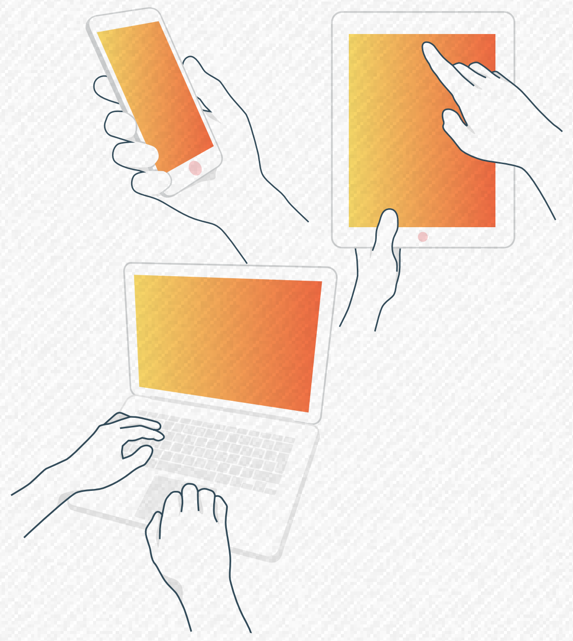
The Network saw a huge spike in digital transactions for the three key shopping dates in November. Consumers seem to be abandoning physical stores in favor of browsing and buying online. Fraudsters tried to leverage this trend; the average basket value of the rejected transactions ~70% more than the overall average.



Up to 10X more traffic than daily average.

Strong growth of transactions from logins (stored credentials/wallets) means that effectively recognizing returning customers is key.

More than 45% of ecommerce transactions were from mobile devices.



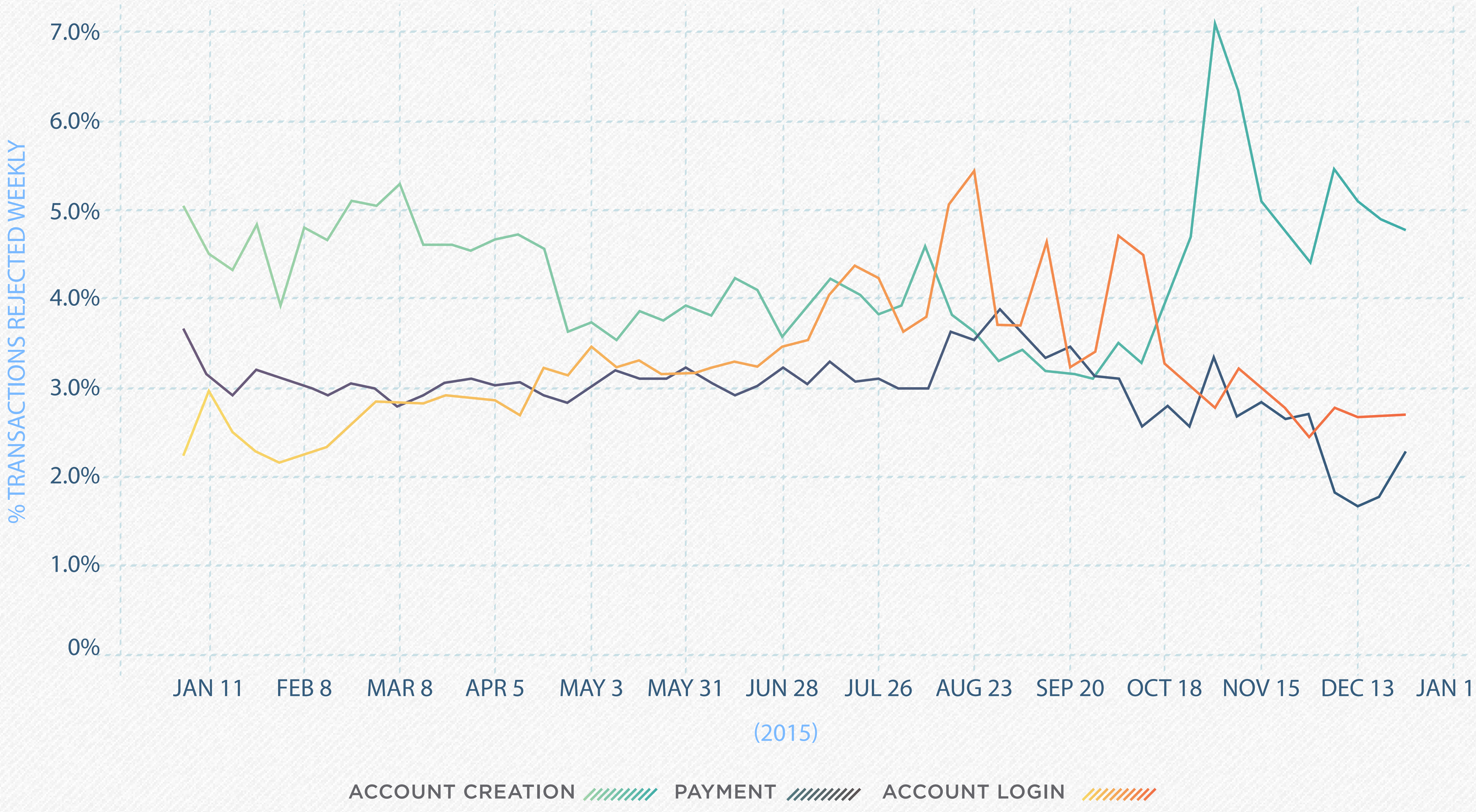
Consumers used multiple devices to shop for deals at trusted retailers.

Higher than average ticket size with customers wanting to buy more items to check off their holiday shopping list. Fraudsters tried to leverage this trend; the average basket value of the rejected transactions ~70% more than the overall average.

RISK TRENDS BY TRANSACTION TYPE

- The impact of recent data breaches is seen globally with steadily increasing attack levels.
- The spike in the new account origination fraud underscores the fact that with the recent data breaches, fraudsters have easy access to sensitive personal information and can use this to open fraudulent new accounts. Static identity assessment methods are no longer effective in verifying a person's true identity.
- This is compounded by the fact that static authentication methods, including credit scoring and address verification, rarely function in a globally connected digital environment. These inadequacies have fuelled sophisticated cyber attacks (such as botnets and malware) that manage to bypass traditional security defenses by mimicking trusted user behavior.
- High legitimate consumer traffic associated with the biggest digital shopping season ever caused the overall attack percentage to be lower than the previous quarter, despite the absolute attacks being the highest to date.

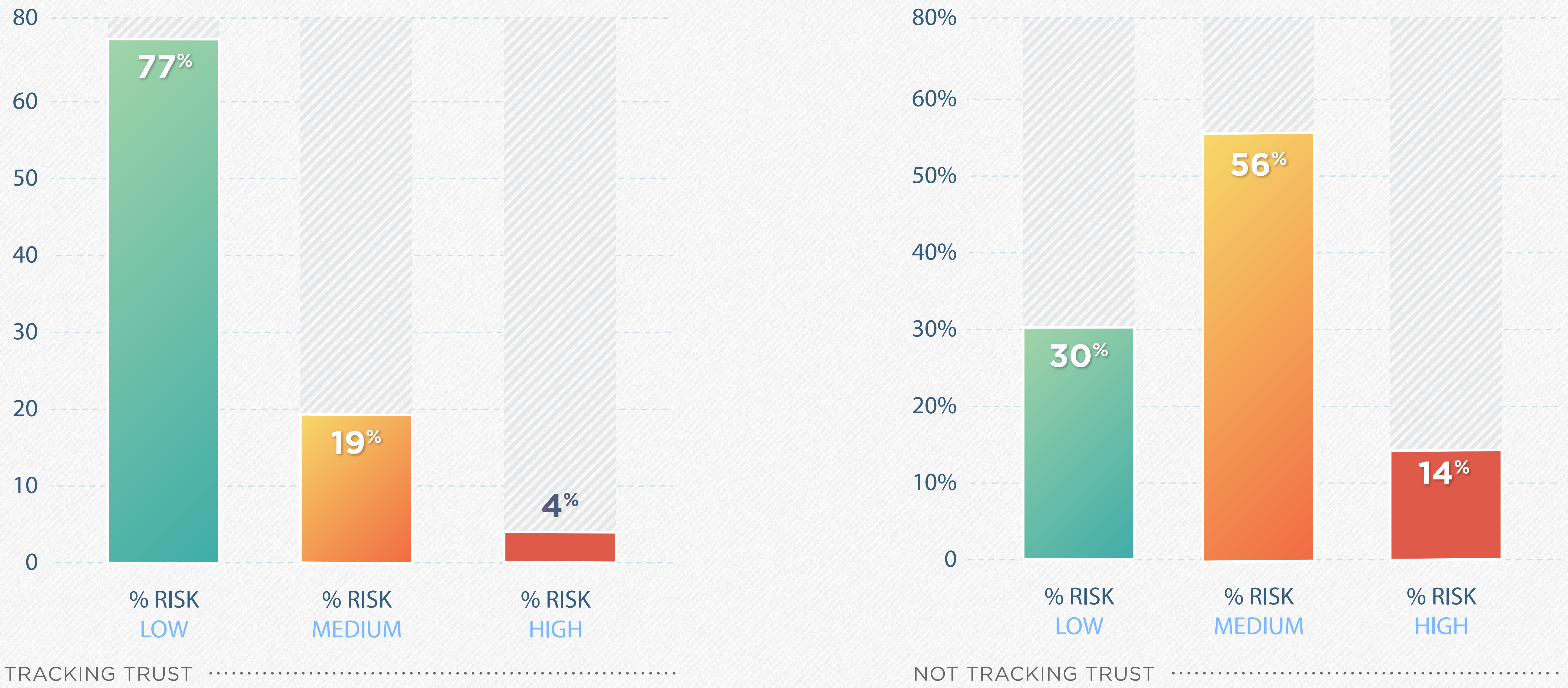
WEEKLY PERCENT REJECTED BY TRANSACTION TYPE



IDENTIFYING TRUSTED USERS

By scoring transactions based on the relative trustworthiness of the user (trust can be associated dynamically with any combination of online attributes such as devices, email addresses, card numbers etc.), businesses can positively identify returning customers and hence deliver an enhanced customer experience with virtually no associated friction.

RISK RATING FINANCE - TRACKING TRUST



Q4 2015 CYBERCRIME REPORT

REPORT OVERVIEW

The ThreatMetrix Cybercrime Report: Q4 2015 is based on actual cybercrime attacks from October 2015 – December 2015 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.

This report also includes a section on the key trends from 2015 based on the billions of transactions analzyed by the Network.

The ThreatMetrix Digital Identity Network provides visibility and insight into traffic patterns and emerging threats. The Network analyzes more than one billion transactions per month, more than a third 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 legitimate end customers’ “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 custom-tuned rules specifically for their businesses.

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

Q4 2015 CYBERCRIME REPORT – KEY HIGHLIGHTS

During this period billions of transactions were analyzed by the ThreatMetrix Digital Identity Network and more than **100 million** attacks were detected and stopped in real time, representing ~80% increase over the previous year. In addition, more than 200 million bot attacks were identified and stopped during this period.

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

- “Digital First” strategies employed by the top retailers and financial institutions are paying off, epitomized by the biggest digital shopping season ever. Consumers are increasingly transacting cross-channel, using connected devices to browse for deals and access products / services.
- Returning users are the biggest drivers of digital transactions. Recognition is critical for conversion and customer loyalty as both financial institutions and retailers strive to establish strong relationship with their users. Organizations must look for ways to reduce friction for trusted users to ensure they are not impacted in the fight against fraudsters.
- Bot attacks continue to be one of the biggest attack vectors for businesses globally.
- In a post-breach world, where sensitive personal credentials are easily available, static identity assessment methods are dead. This is compounded by the evolution of highly sophisticated cybercrime tactics such as botnets and malware attacks that manage to bypass traditional security defenses by mimicking trusted user behavior.

TRENDS

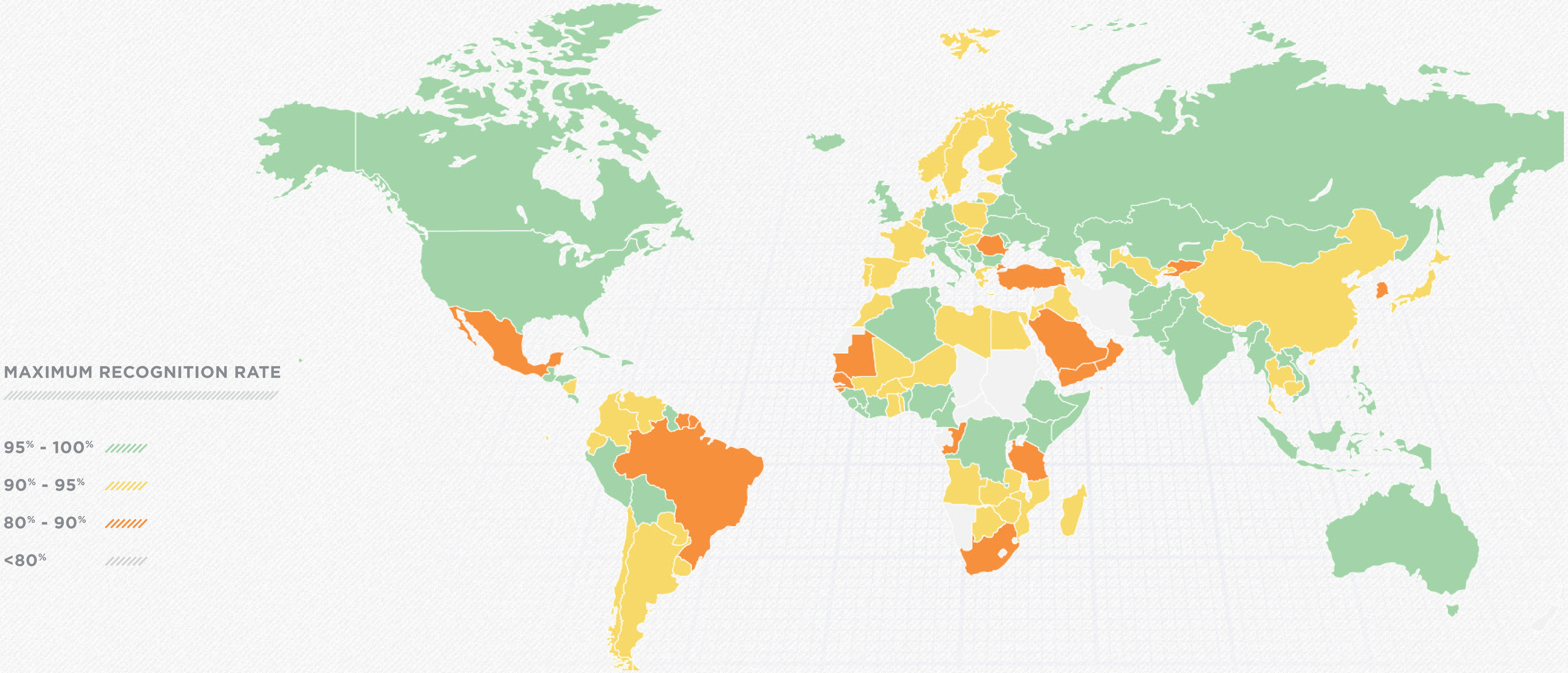
- Biggest digital quarter ever with multiple periods of strong activity including China's Singles Day, Black Friday and Cyber Monday.
- Consumers continue to access e-commerce, media and financial services through multiple devices.
- Loyalty and trust is key with most e-commerce transactions coming from repeat customers.
- 80% increase in attacks over Q4 2014; and 250% increase in attacks on retailers during the peak shopping days.
- Transactions originating from desktop continued to be attacked more.
- Cybercrime is a global phenomenon with fraudsters targeting businesses in the countries with high online and mobile penetration.

SURPRISES

- Growth of digital transactions at the expense of in-store sales.
- Key peaks in digital transactions around midday and 9pm. Online shopping fits into the natural rhythms of a customer's day rather than working round store opening times.
- Growth in new account origination fraud targeting Financial Institutions.
- The relentlessness of bot attacks that are designed to evade Web Application Firewalls (WAFs) and rate control protections. The network detected 230 million bot attacks.
- Attackers are increasingly targeting emerging economies with high mobile deployment. India featured as the top attack destination for the first time.

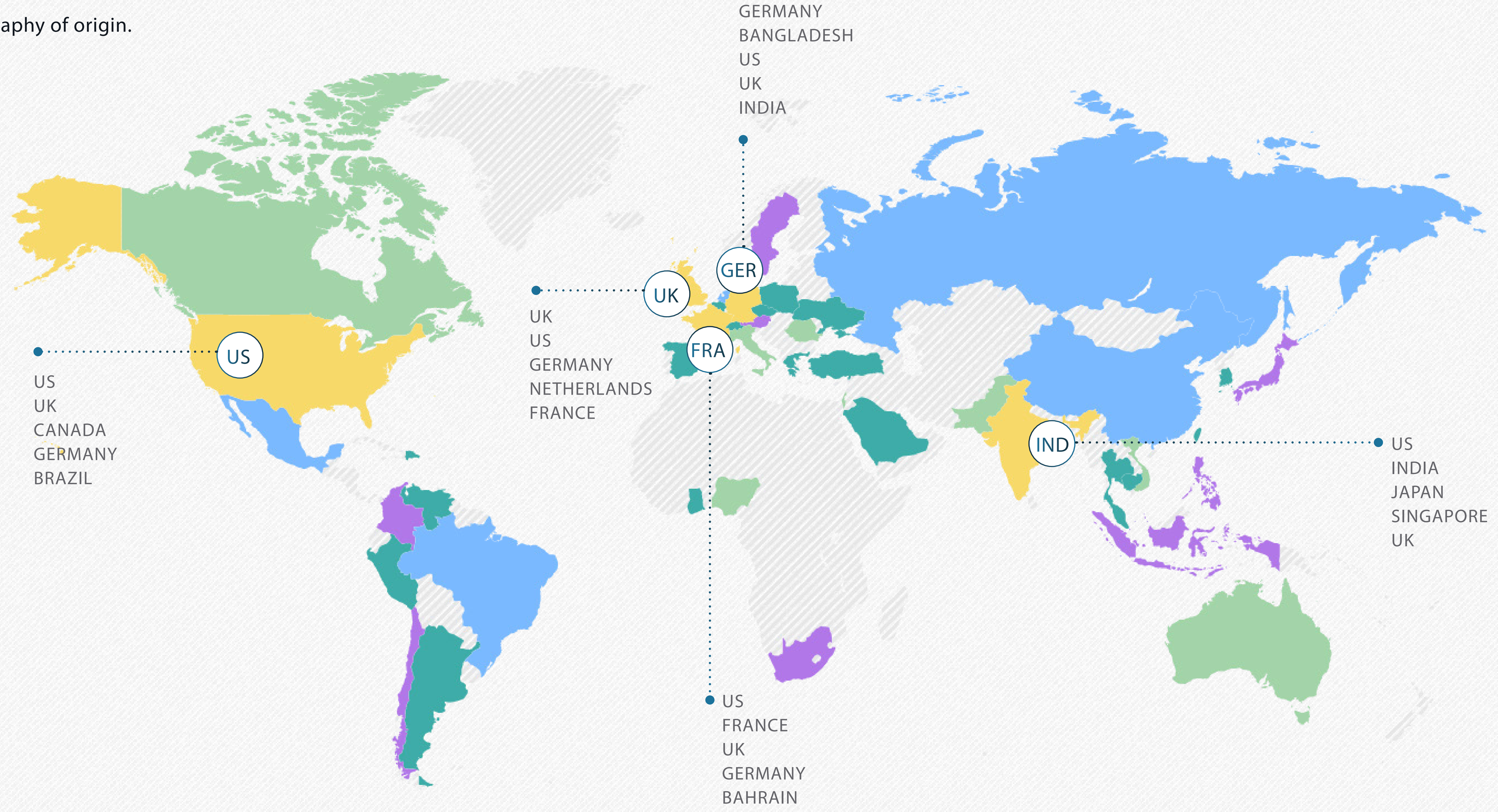
RECOGNITION IS KEY

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.



ATTACK ORIGINS BY GEOGRAPHY

Total number of attacks detected by geography of origin.



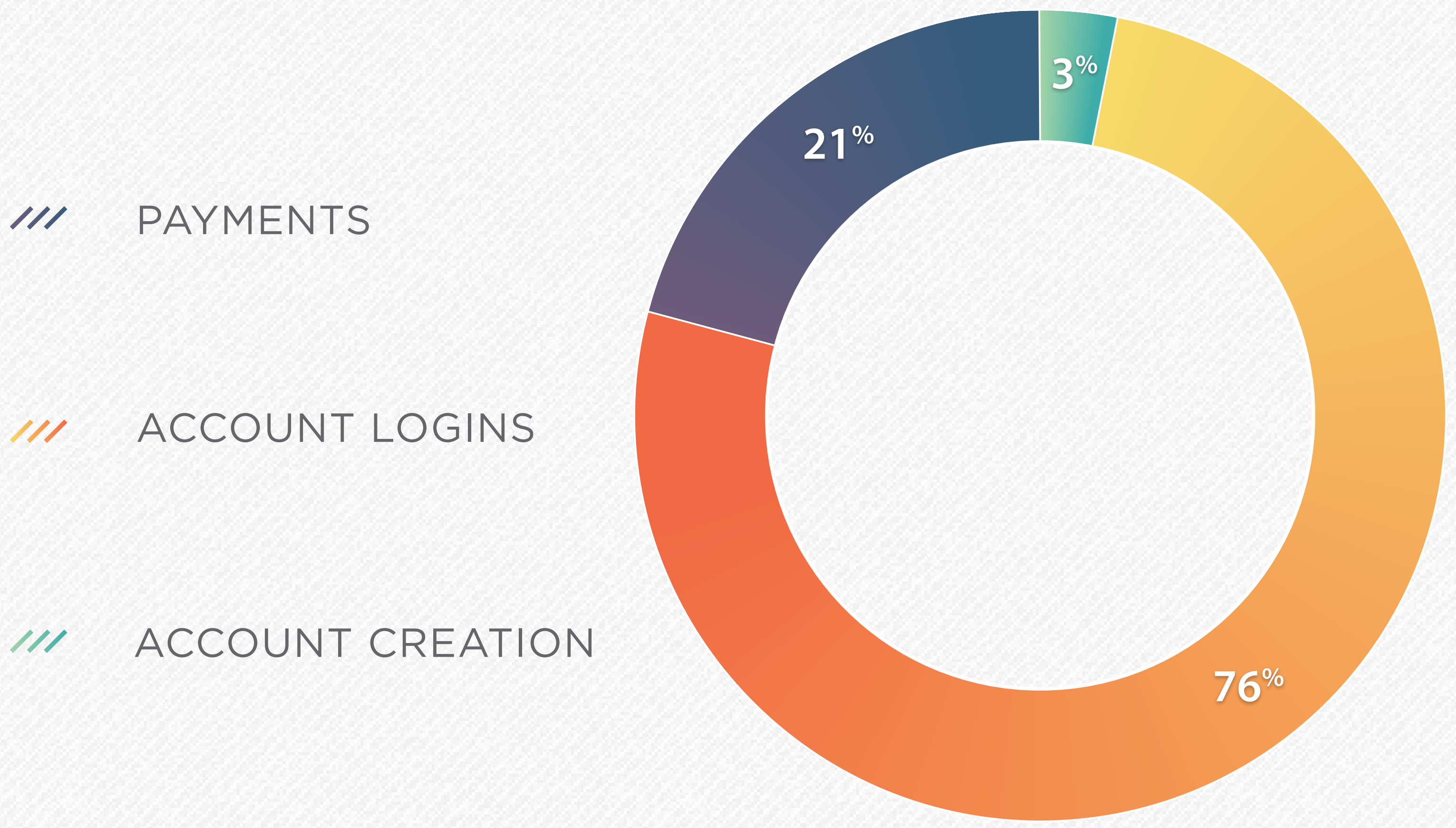
COUNTRY RANKING

Top 5	▨
Top 6 - 10	▨
Top 11 - 20	▨
Top 21 - 30	▨
Top 31 - 50	▨
Top 50+	▨

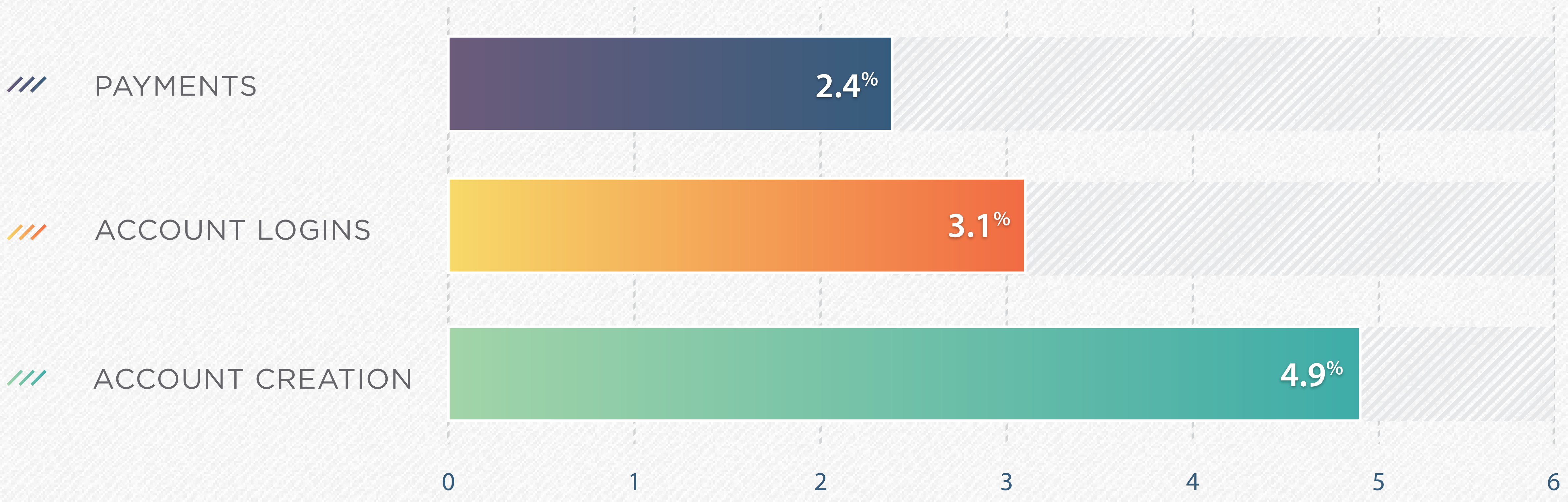
TRANSACTIONS ANALYZED BY TYPE

- ThreatMetrix transactions span e-commerce, 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 businesses deploy ThreatMetrix to verify their users' digital identities without impacting consumer experience.
- There was a large increase in account creation and account takeover fraud driven by the increased availability of stolen identities in the wild, harvested from massive breaches. The overall attacks increased by over 100% compared to the previous year.
- Financial services organizations are less likely to block suspicious transactions outright, subjecting them instead to further review.

VOLUME BY TRANSACTION TYPE



ATTACKS BY TRANSACTION TYPE

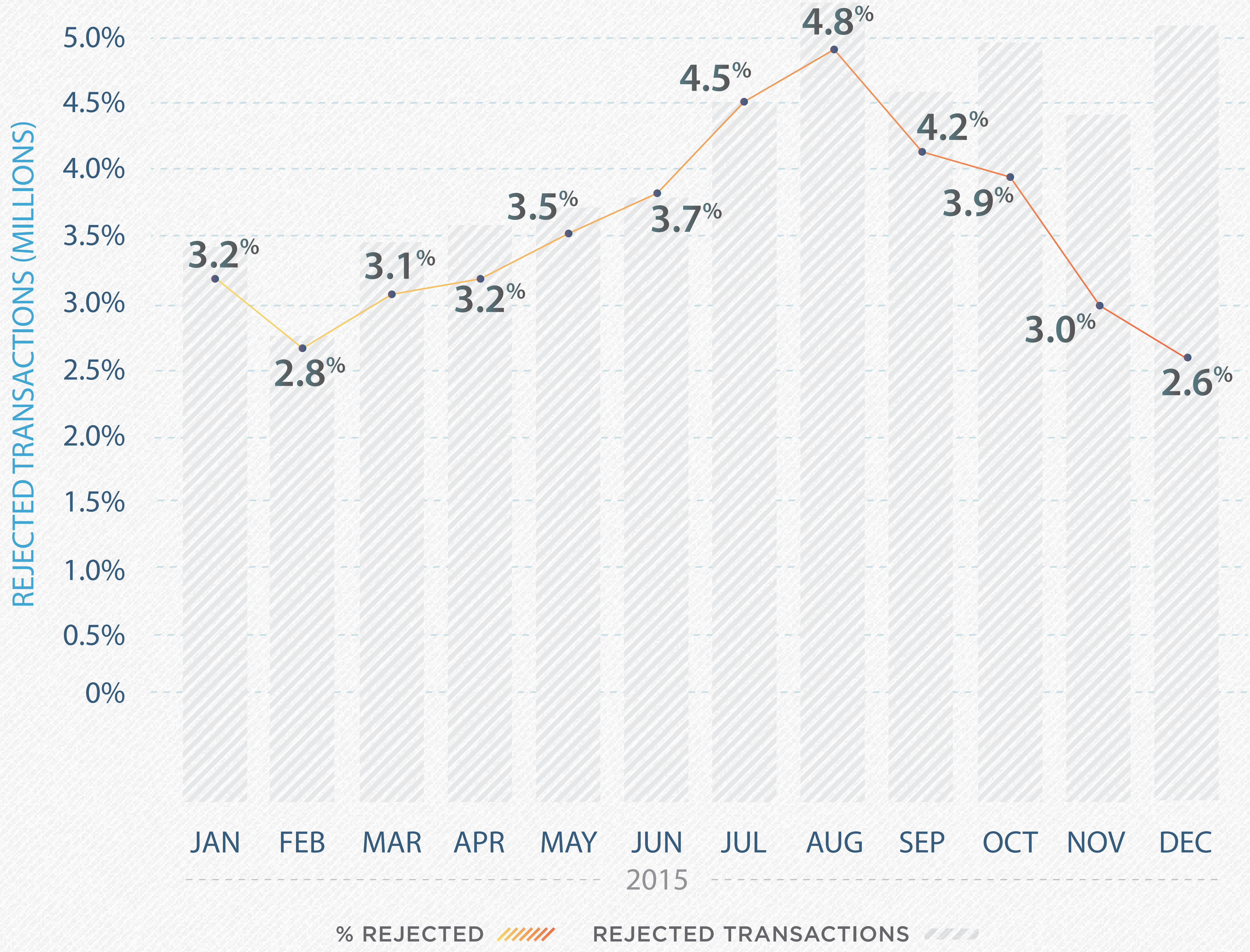


__Attack percentages__ are based on transactions identified as high risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically in real time dependent on individual customer use cases.

RISK TRENDS BY TRANSACTION TYPE

- The 2015 Cybercrime Christmas season saw the highest ever attacks across transaction types. Roughly 28 million fraud attempts targeted online retailers during the peak shopping period; these attacks represented ~250% increase over the same period in 2014.
- The Q4 shopping season saw an unprecedented growth of digital transactions. This caused the overall percentage of rejected transactions to drop off despite the fraud levels being highest ever.
- This period also saw a high level of bot attacks looking to run massive identity verification sessions on the big retailers.

ATTACKS PER MONTH (% AND COUNT)



E-COMMERCE TRANSACTIONS AND ATTACKS

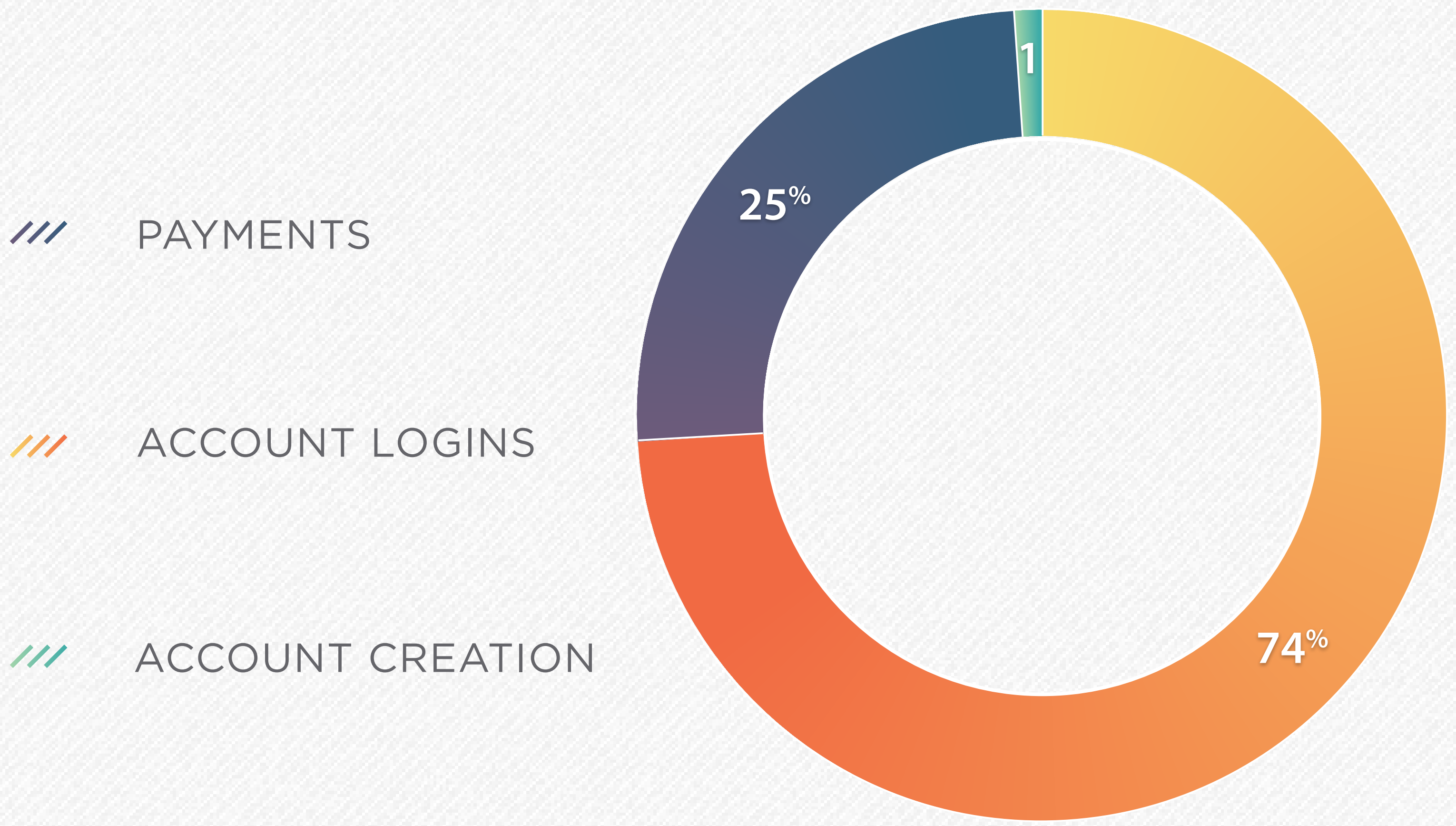
The holiday season is the grand finale of the digital story that had been playing out for the past few years. While attacks and threat levels remain high, the big focus across industries is to deliver a slick and frictionless experience to customers as they browse online for deals and discounts.

Spending in stores fell 10% from last year on both Thanksgiving and Black Friday, according to retailing research firm ShopperTrak.

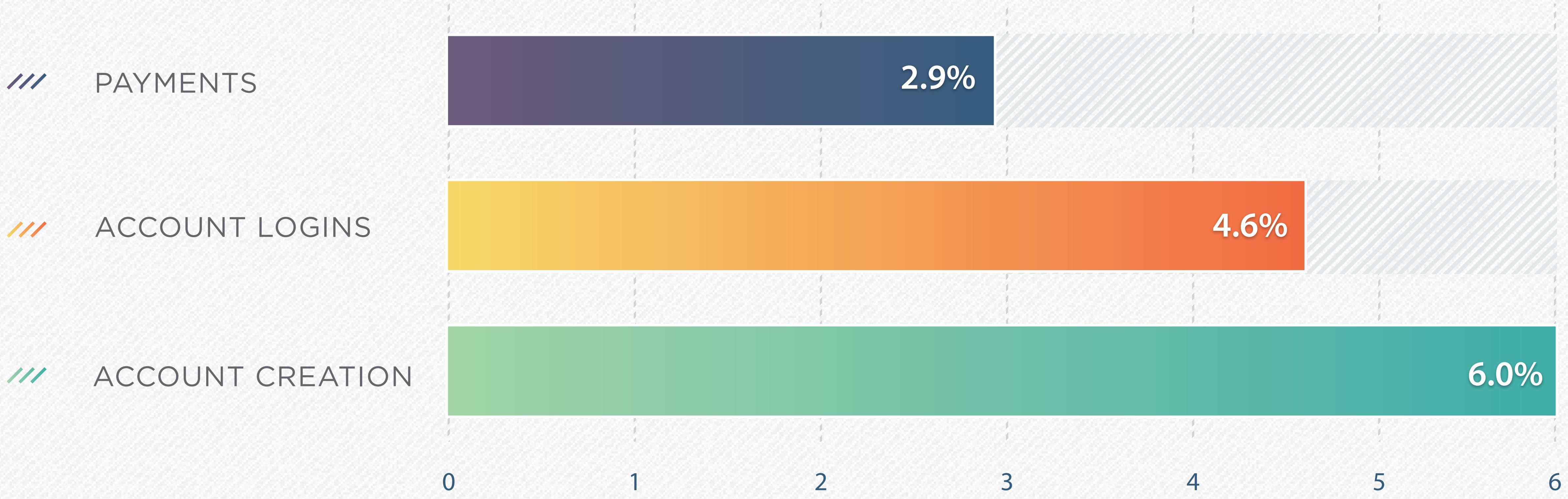
Login transactions remain high but there was also a significant volume of payment transactions. More attacks for login and payment events were detected in this period, consistent with the seasonal shopping spike. Overall the network detected ~58 million attacks during this period, a 25% increase over the previous quarter and ~124% increase over last year. This signifies billions of dollars in potential financial loss, as well as damage to brand reputation, that has been avoided.

The biggest impact of cyber attacks was seen on the new account origination transactions, as fraudsters used new accounts to make purchases using stolen credentials. These transactions increased by over 133% and the attacks grew by 180% compared to last year. With consumer identity data widely available due to recent breaches, traditional identity assessment methods are becoming ineffective.

VOLUME BY TRANSACTION TYPE



ATTACKS BY TRANSACTION TYPE

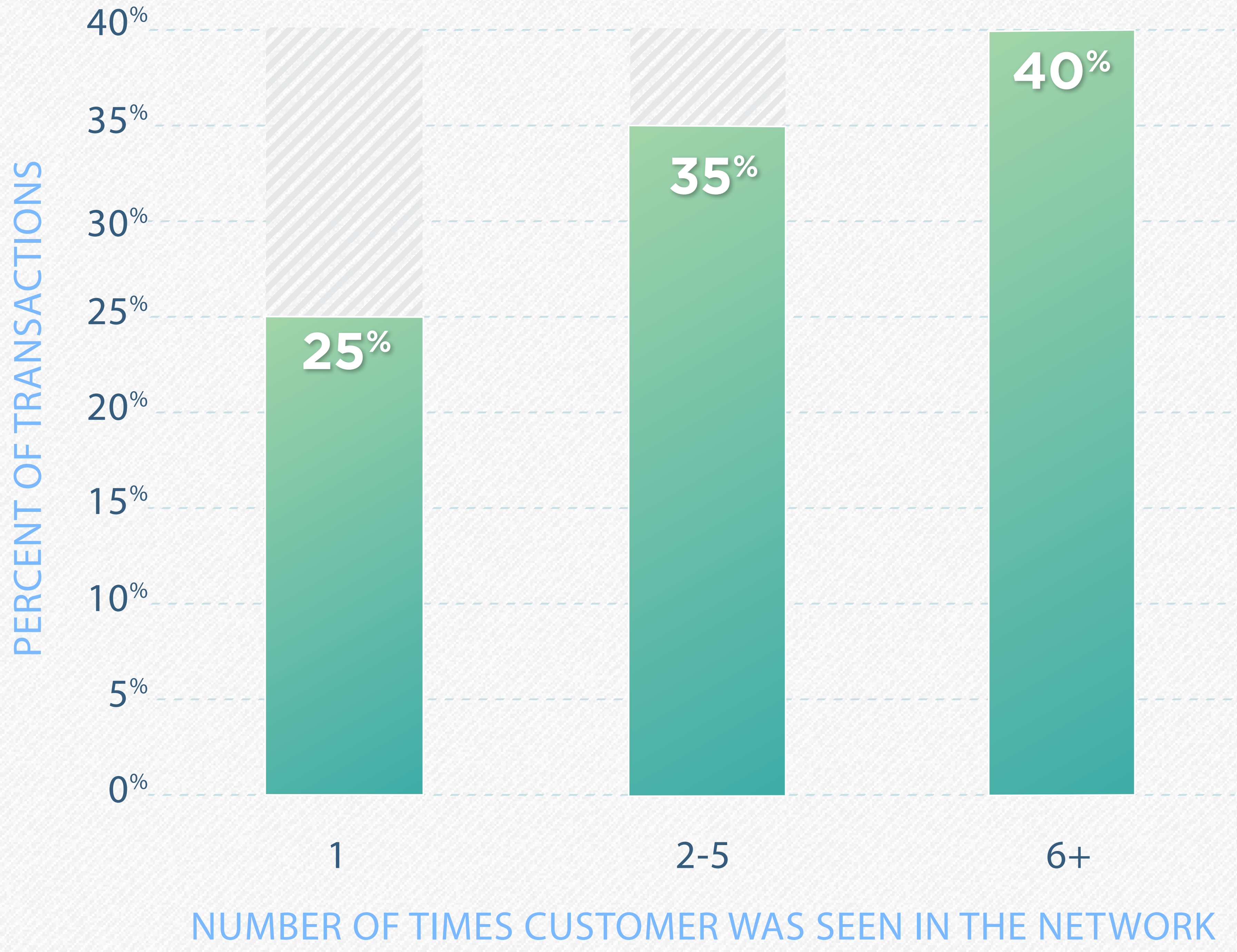


E-Commerce includes retail, airlines, gambling, gaming, travel, marketplaces, ticketing and digital goods businesses.

HOLIDAY SHOPPING – TRUST IS CRITICAL

- Consumer activity intensified during the week leading up to to Cyber Monday as retailers began offering deals ahead of the peak shopping days.
- Of the 292 million transactions analyzed during this period, 75% of these came from consumers who were seen in the network more than once and 40% more than 5 times.
- Recognition is key to stopping fraud without impacting customer experience.
- Amidst huge shopping volumes, we continued to recognize ~85% of all returning customers' devices, which helped keep friction low for trusted customers.
- We also were able to rate ~90% of the customers as low risk, which helped businesses deliver great customer experience without adding friction.

TRANSACTIONS ANALYZED FROM NOV 24 – NOV 30



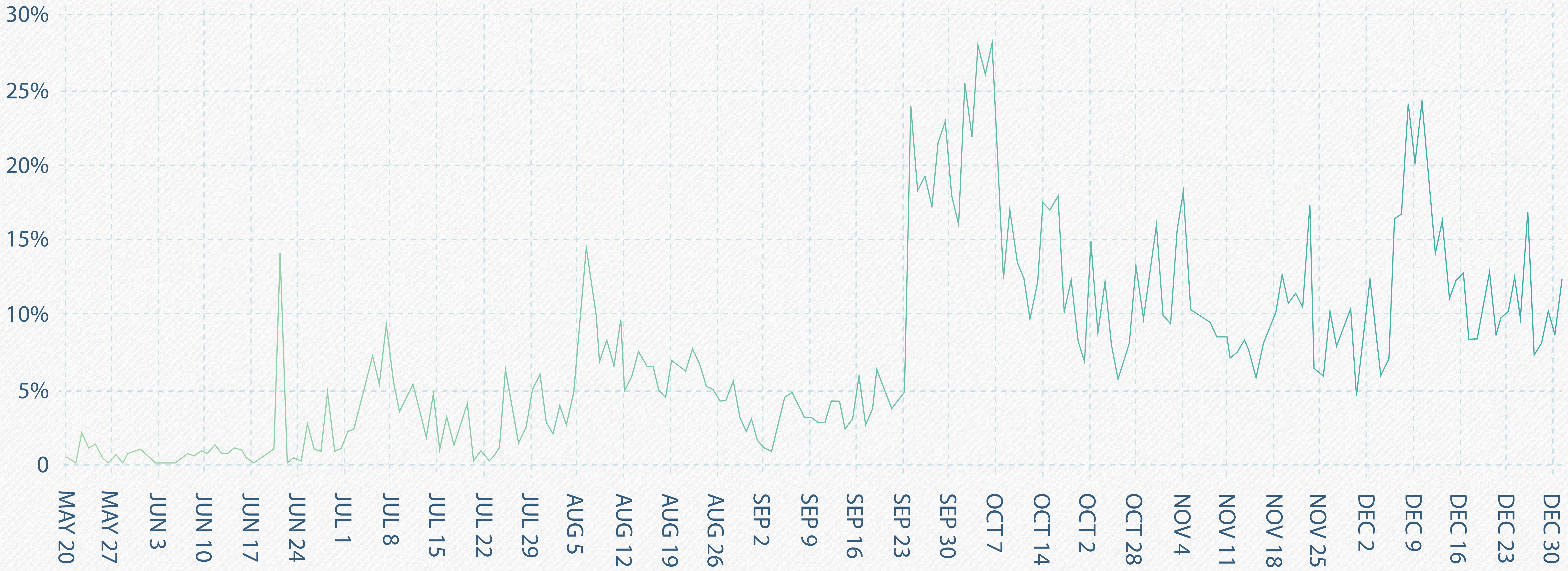
WEB ATTACKS EVOLVING TO EVADE EXISTING CONTROLS

Web attackers are becoming more sophisticated, attempting to evade existing security controls. For example bots and botnets have developed a low-and-slow attack rate designed to evade rate and security control measures and mimic trusted customer login behavior, making them much harder to detect. Digital businesses face very high daily traffic due to these automated botnet attacks launching huge identity testing attacks to try and gain access to customer accounts.

Logins are rapidly becoming a leading use case for retailers as they seek to establish meaningful relationships with their customers. These bot attacks are effectively the precursor to actual fraud attempts, as fraudsters seek to test whether they can access customer accounts.

ThreatMetrix uses context-based information to perform behavioral analysis of users during periods of normal operation and compares such data to that gathered during a slow-rate attack. This enables ThreatMetrix to differentiate between a human and a bot the moment they land on the site.

PERCENT TRANSACTIONS SEEN AS BOT ATTACKS - E-COMMERCE



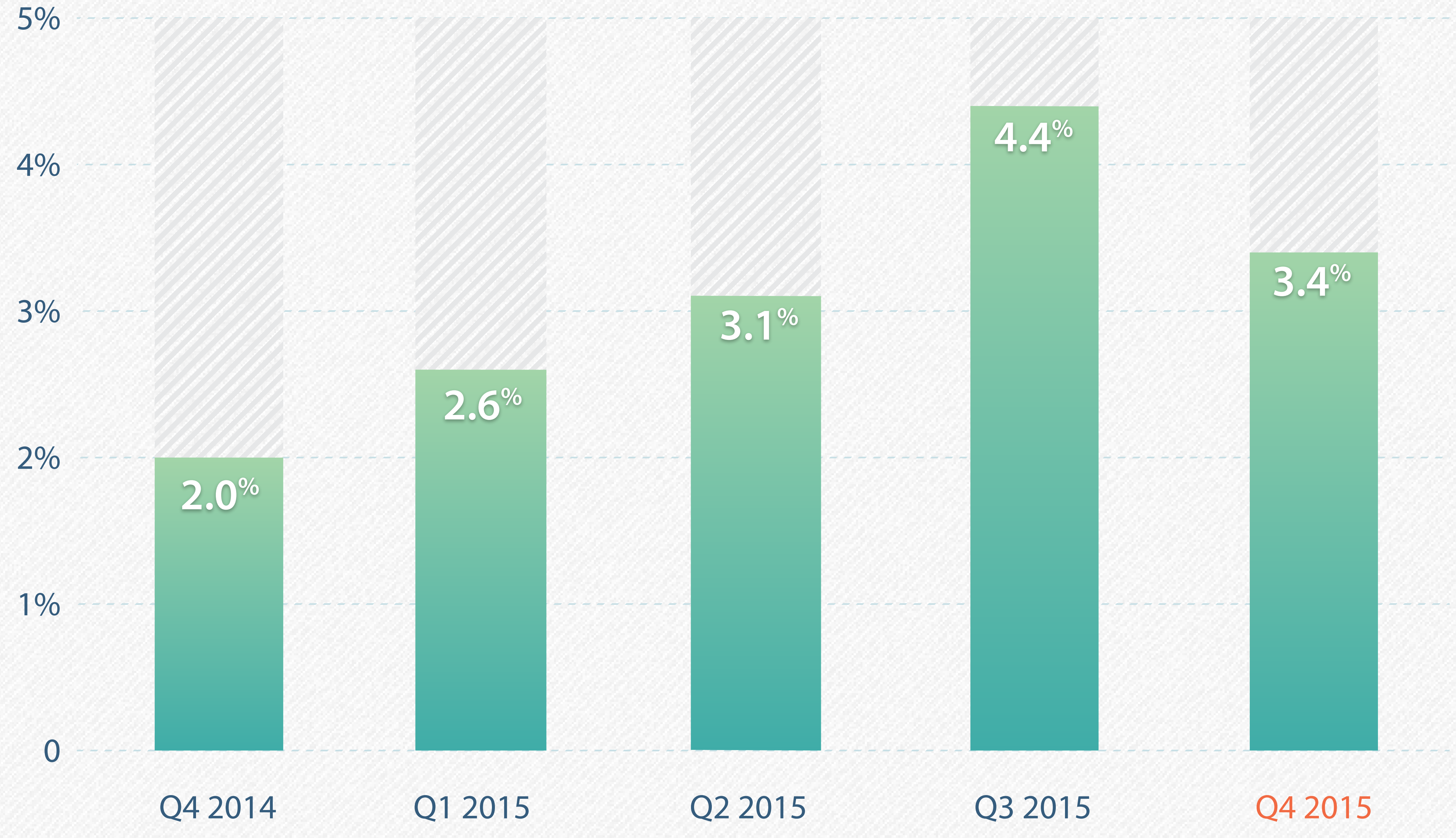
ATTACKS ON ONLINE RETAILERS GROWING RAPIDLY

- Attacks on e-commerce transactions have steadily increased over the last year. With the migration to EMV in the U.S., these attacks will continue to be high.

- Despite the decline in the overall percentage of rejected transactions, the total attacks in Q4 went up by 30% over Q3 2015 and 124% over the previous year. This was due to a massive increase in digital transactions.

- Retailers are working at building strong customer relationships, leading to more customers having accounts rather than making one-off purchases. This has had a knock on effect on login attacks, which are also growing largely as a result of bots. Identity is now a much more lucrative target compared to individual transactional attacks.

PERCENT REJECTED

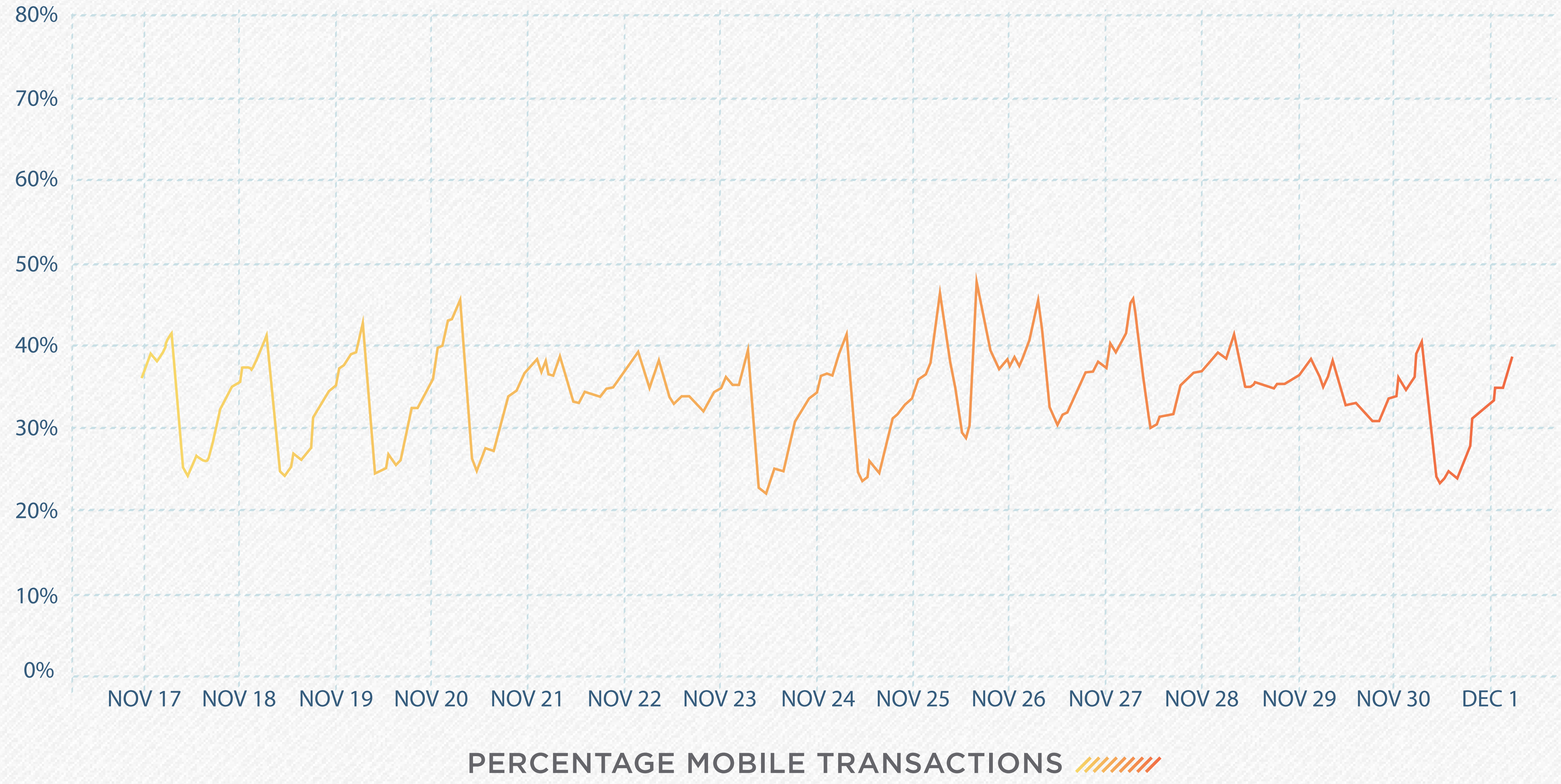


2015 HOLIDAY STATISTICS – USAGE AND GROWTH

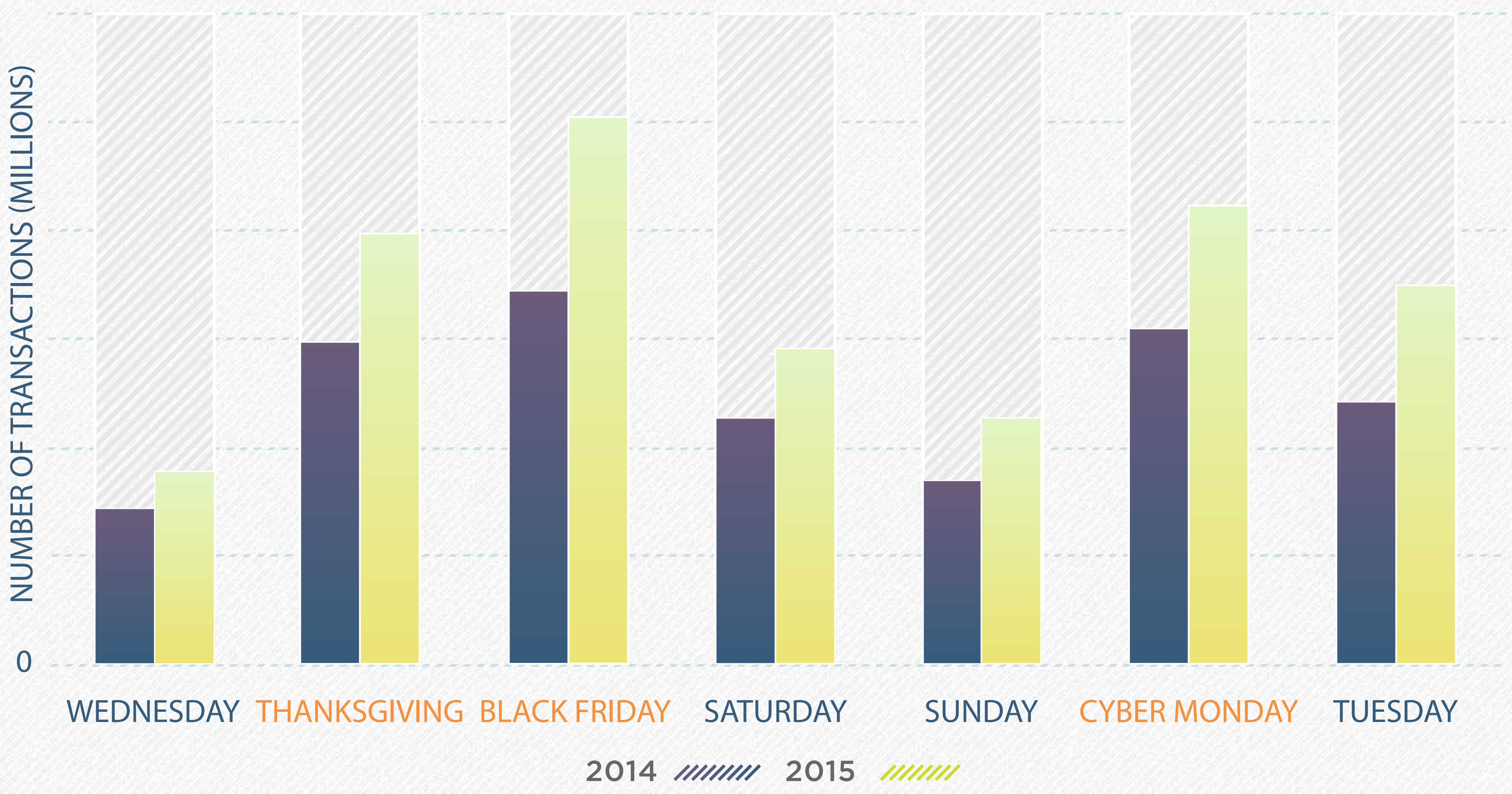
The concept of Black Friday has become more of a sales tactic and has lost its relevance as retailers begin offering deals in the days leading up to and past thanksgiving. Despite this, The Network saw significant growth compared to the top retailers' 2014 shopping volume for the same days.

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

HOURLY MOBILE VERSUS DESKTOP TRANSACTIONS



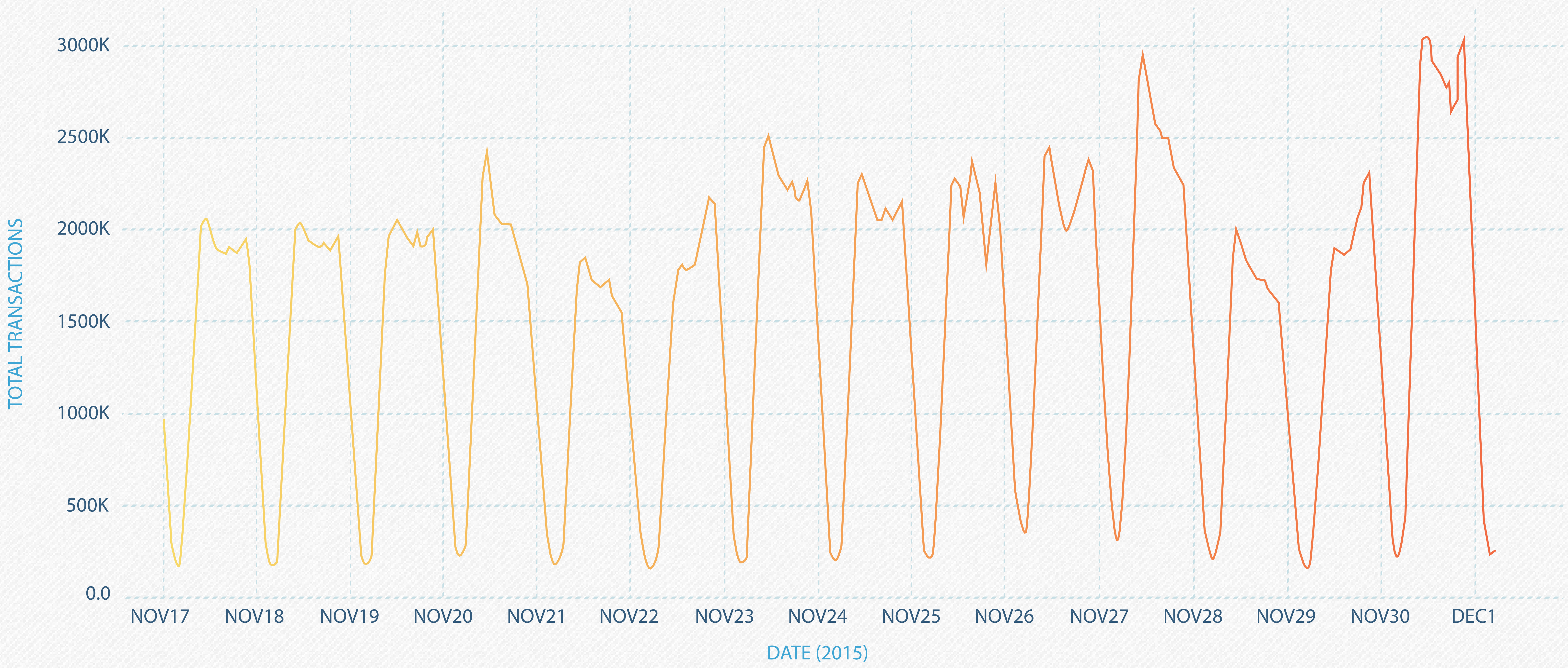
TRANSACTION VOLUME THANKSGIVING HOLIDAY WEEK 2014-2015 (TOP RETAILERS)



2015 HOLIDAY STATISTICS – HOURLY TRANSACTIONS

- The increased digitization of consumers also created multiple "peaks" throughout the day across the key shopping days.
- As more and more retailers are embracing "digital first" strategies, many deals are now available online which negates the need to go to a physical store. However, the lure of getting these deals before anyone else still prevails, seen in the spikes right at midnight as consumers make a transaction just as an offer goes live. We observed high volumes throughout the big shopping days with peaks being around midday and late evening.

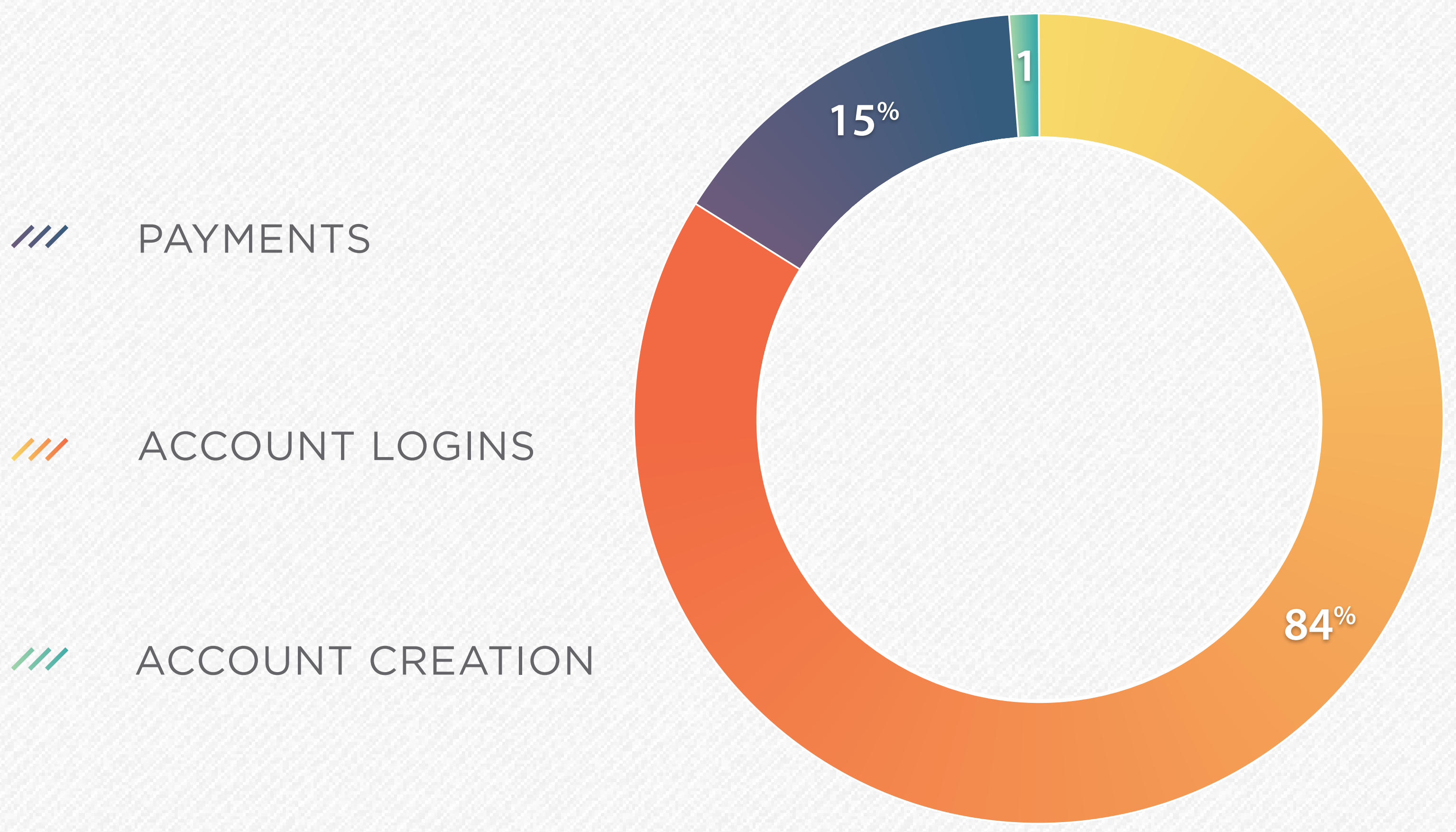
HOURLY TRANSACTIONS LOCAL TIME



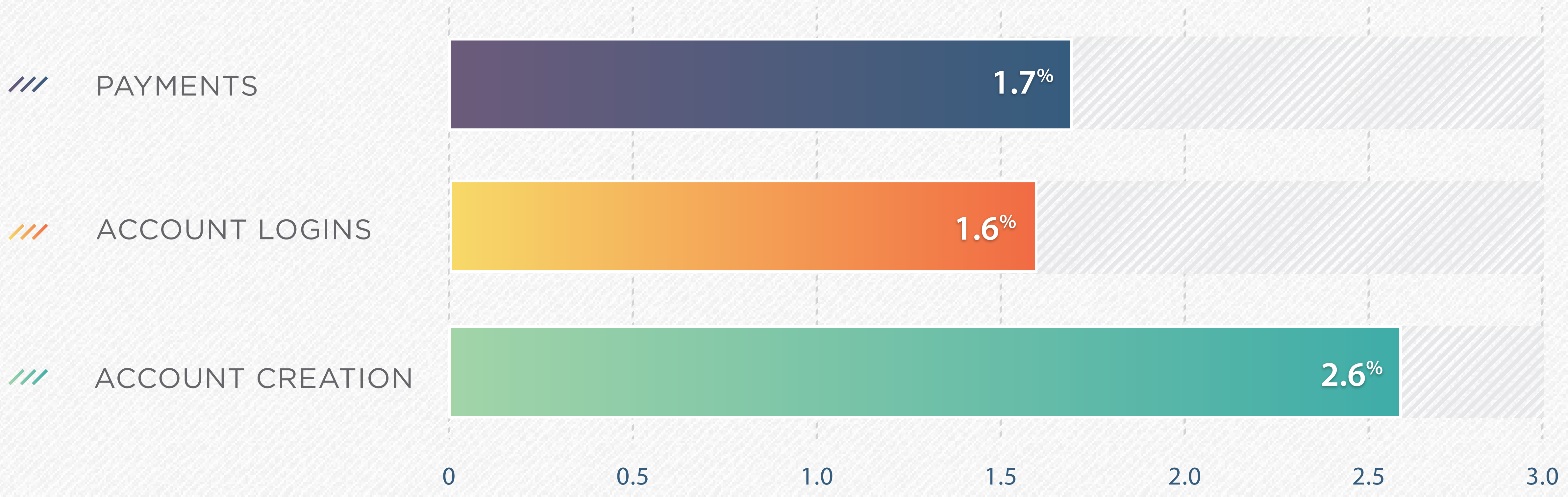
FINANCIAL SERVICES TRANSACTIONS AND ATTACKS

- Financial institutions continue to be big targets for organized attacks and face multi-channel threats from the same location or simultaneous attacks on a single access point from multiple locations across the globe.
- The migration to EMV in the U.S. was expected to result in an increase in new account origination fraud which was evident in the holiday season. ThreatMetrix detected and stopped over 21 million attacks during this period, a 40% increase over last year.
- Login transactions grew this period as consumers validated their accounts often during the holiday season. While login attack percentages are low, the risk exposure due to illegal money transfers and potential brand damage is high. Login transactions are big targets for bot attacks aimed at testing stolen identities. ThreatMetrix detected and stopped an additional 45 Million bot attacks during this period.
- Mobile share of transactions grew significantly over the previous quarter as more and more shoppers accessed their mobile banking apps to check balances during the holiday shopping period.

VOLUME BY TRANSACTION TYPE



ATTACKS BY TRANSACTION TYPE

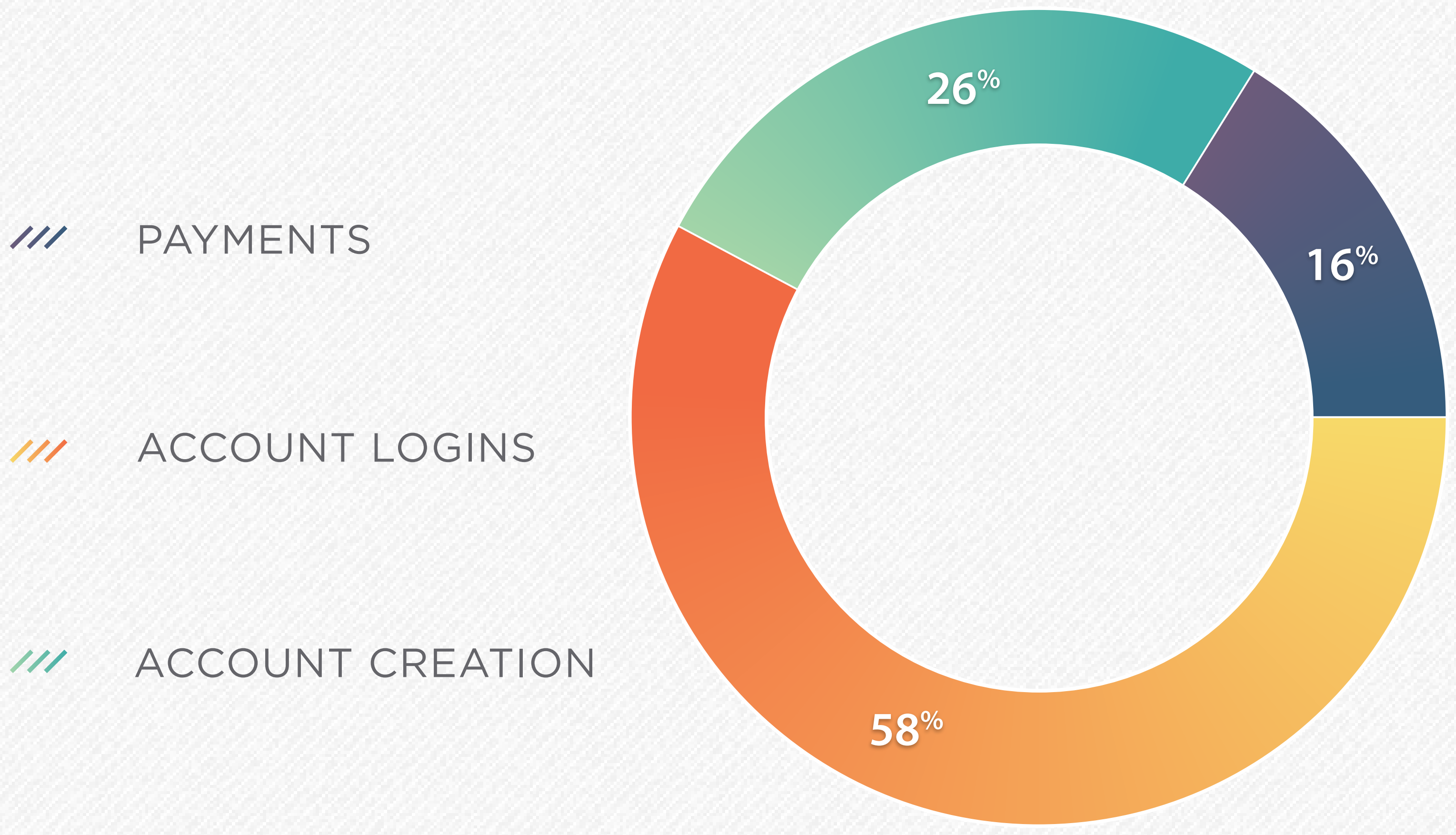


__Financial Services__ includes mobile banking, online banking, online money transfer, lending, brokerage and credit card issuance.

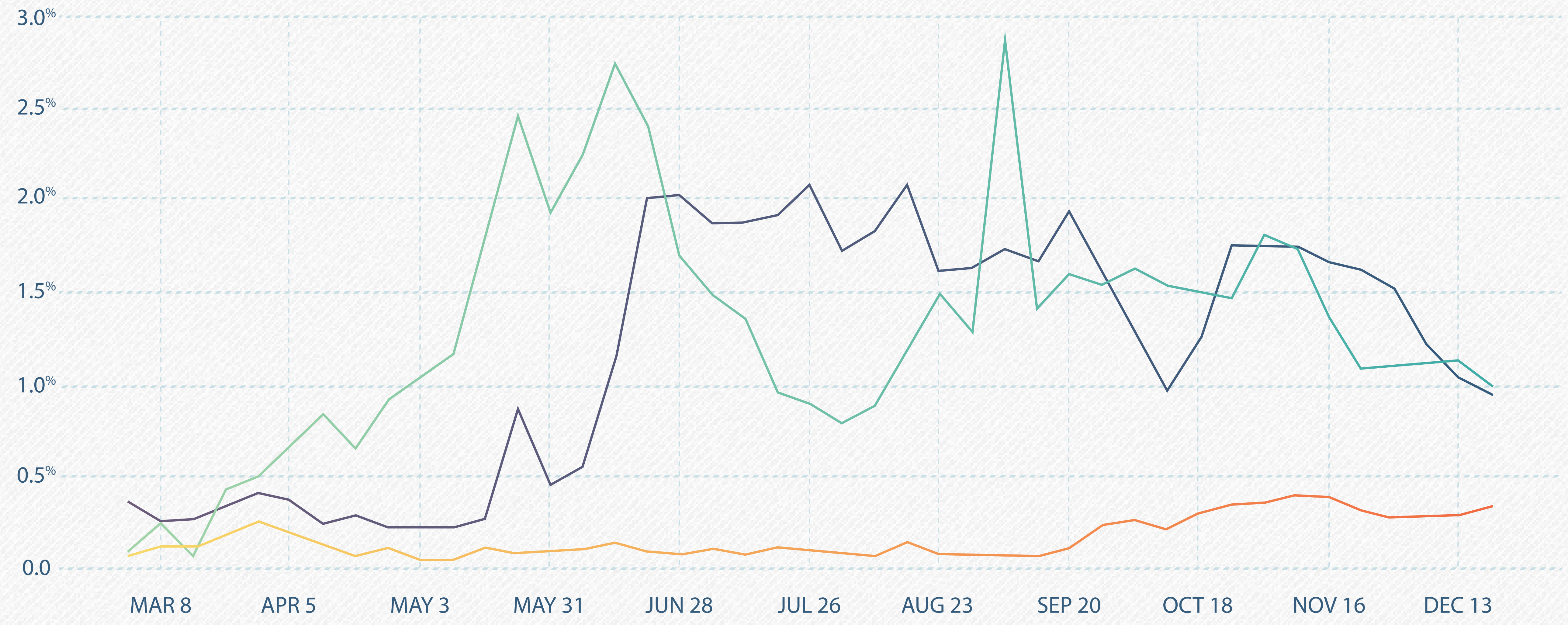
ONLINE LENDING AND ALTERNATIVE PAYMENTS

- Digital commerce is providing a launch platform for small or niche businesses that previously struggled to keep up with the established players. Internet-only banks, small lenders and niche insurance brokers are innovating to meet the evolving needs of digital consumers including the unbanked and underbanked population, who previously had little access to traditional banking services.
- New account creation and payments represents a very high percentage of transactions for this channel compared to the traditional banking segment. Since these events represent significant financial benefit, this segment is continuing to experience a very high volume of attacks.
- The overall attack levels grew compared to the previous quarter driven by an increase in new loan applications ahead of the holiday shopping.

VOLUME BY TRANSACTION TYPE



ONLINE LENDING PERCENT REJECTED MONTHLY PER TRANSACTION TYPE



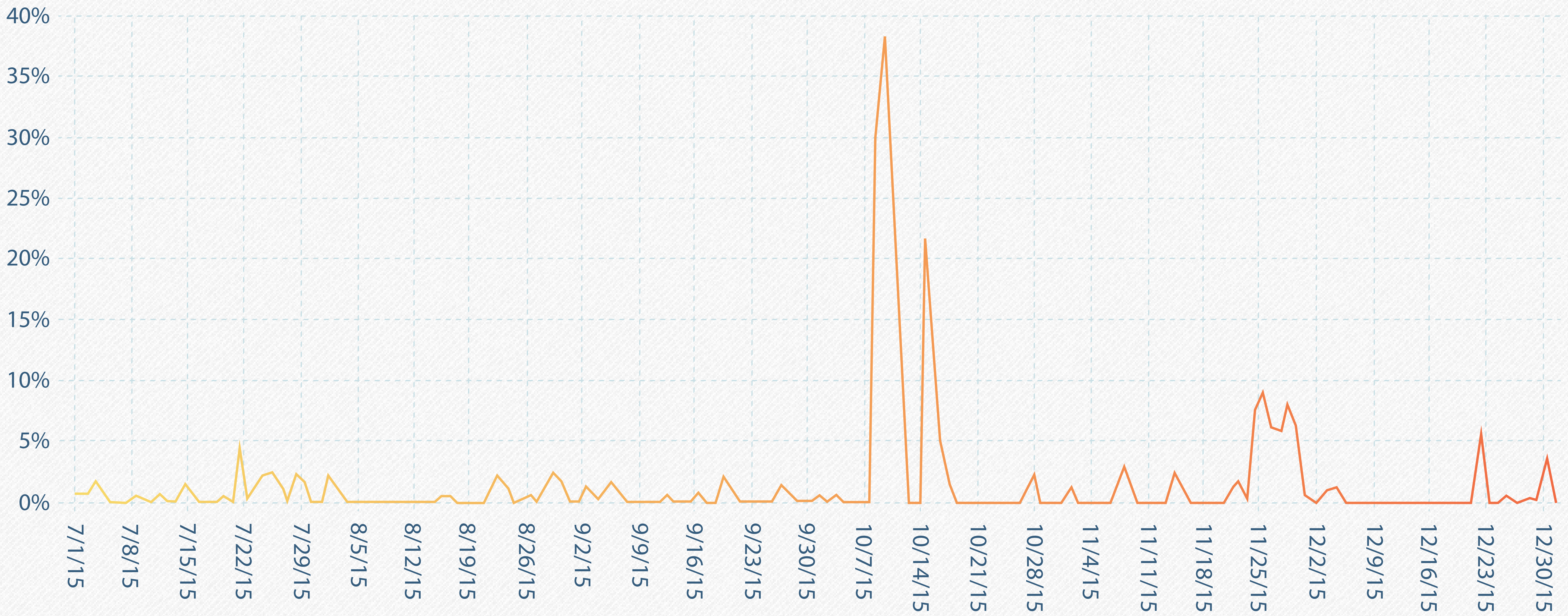
EMERGING ATTACK VECTORS

Cyber attacks are growing in size, complexity and risk and one of the big drivers of this is the massive growth in malware targeting individuals and businesses alike.

Fraudsters have large-scale networks of infected devices available at their disposal to inundate online systems with large volumes of fraudulent transactions. They also use scripts (often in conjunction with bots) to perpetrate such transactions.

ThreatMetrix detected millions of credential testing attempts using bots / scripts that targeted financial institutions, almost 10 times the volume from the previous quarter. An increase of such testing almost always occurs following a large scale data breach.

DAILY PERCENTAGES OF TRANSACTIONS COMING FROM BOTS - FINANCE



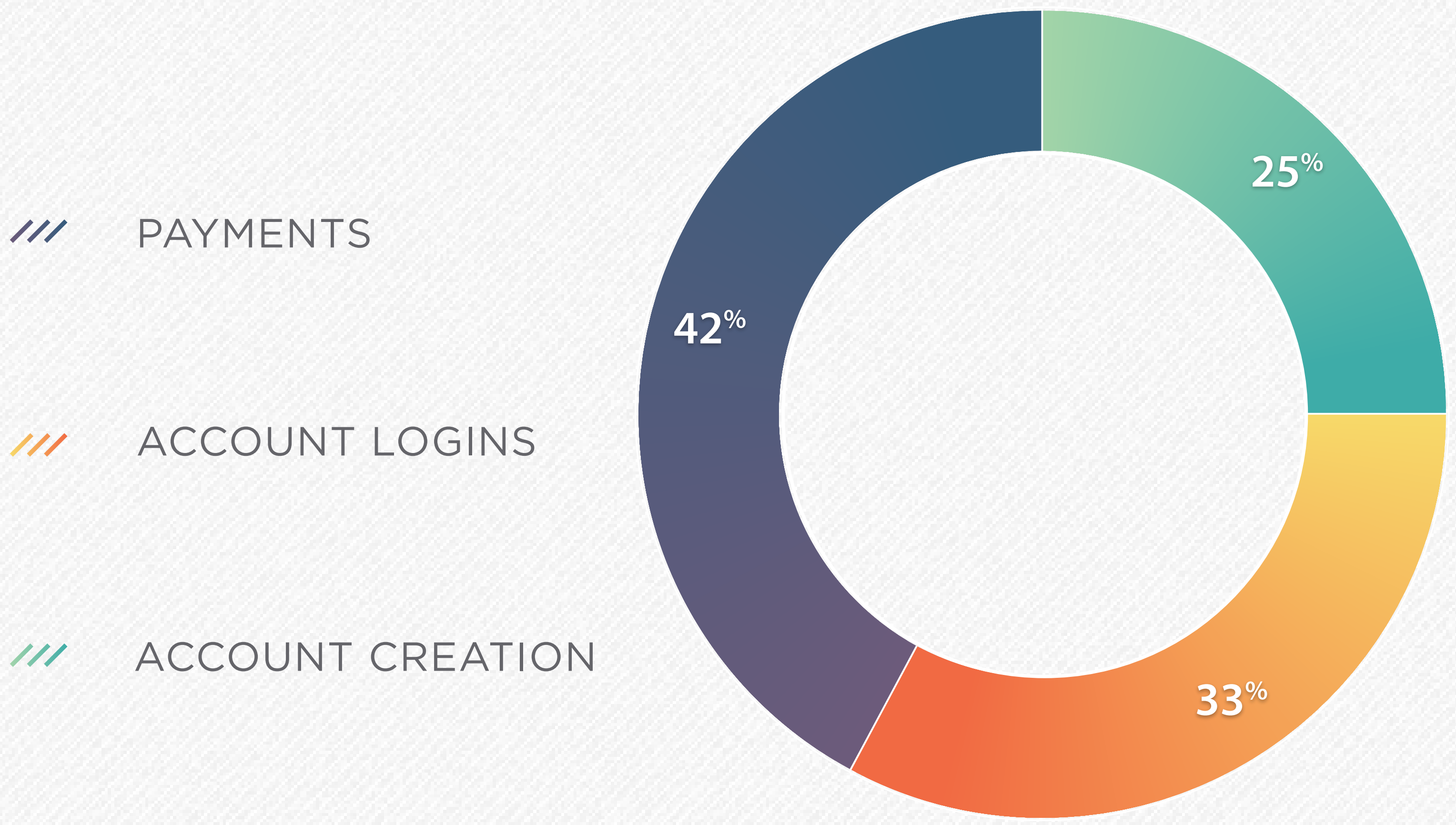
MEDIA TRANSACTIONS AND ATTACKS

Attacks on media transactions continue to be higher than any other segment. Media volumes have grown steadily over the past few years as more and more content is made available "on-demand" through digital channels.

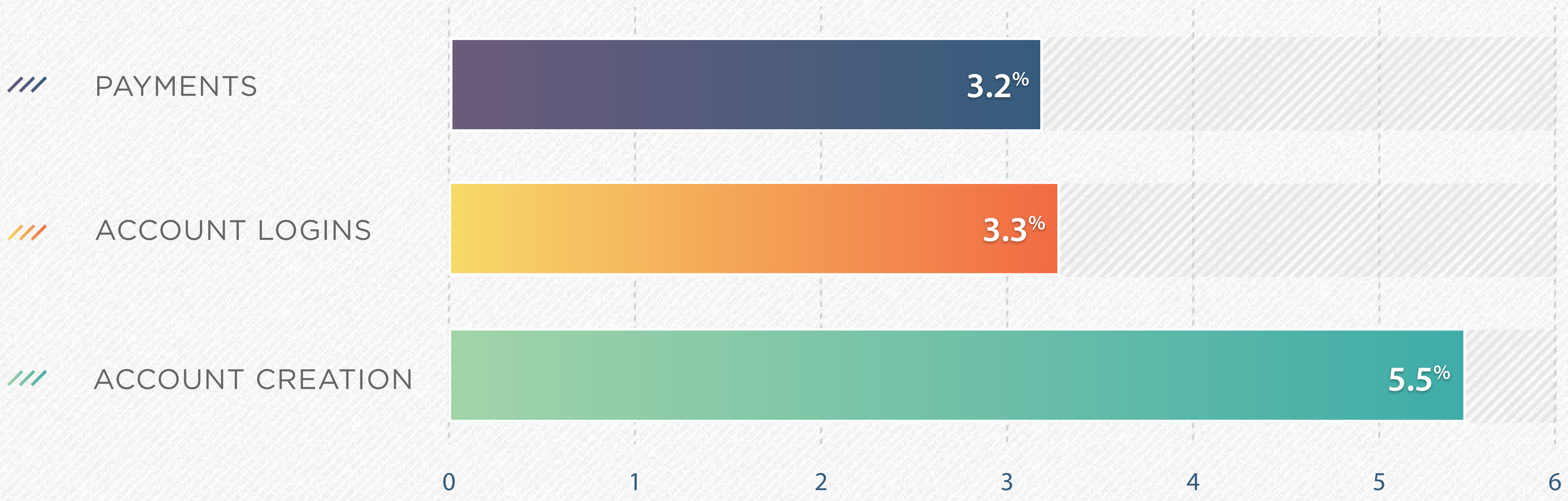
As businesses struggle to balance consumer experience with fraud prevention, fraudsters attempt to leverage deals and offers by creating bogus accounts. Modest sign-up and authentication requirements makes digital media, social networks as well as content sharing businesses easy targets for fraudsters looking to test the validity of the stolen credentials. Spamming and fraudulent account creations continue to be a big driver of fraud. This quarter saw a 66% increase in fraudulent new account registrations.

Reviews and feedback are the backbone of the shared economy and prospective users rely on these to make their purchase decisions. ThreatMetrix detected and stopped millions of fraudulent reviews and listings during this period.

VOLUME BY TRANSACTION TYPE



ATTACKS BY TRANSACTION TYPE

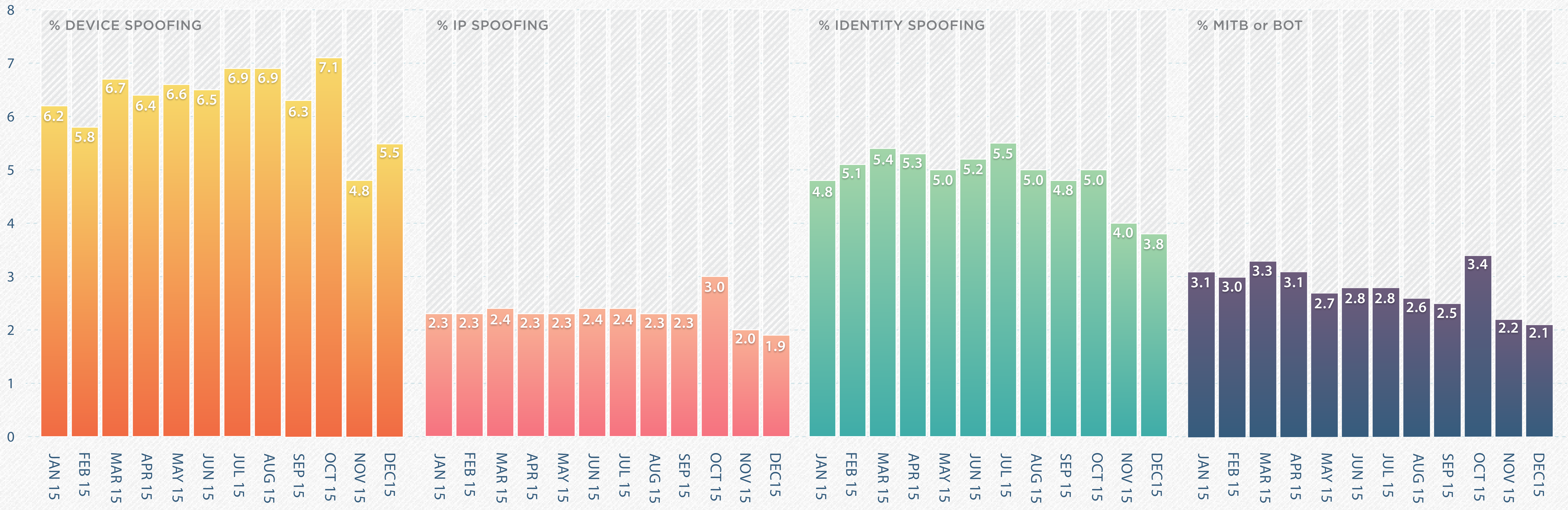


***Media** includes social networks, content streaming and online dating sites.*

TOP ATTACK VECTOR TRENDS

- Attack vectors are analyzed in real time by the ThreatMetrix global policies. Some attacks use multiple vectors. Device spoofing remains the top attack vector with identity spoofing growing rapidly.
- Fraudsters either replay stolen identities using proxies, spoofed devices, and location spoofing to cloak their true digital identity, or piggy-back a user's session with malware or man-in-the-middle attacks.
- Criminals are increasingly stitching together the various aspects of consumer data made available through breaches to open new accounts, steal payment information and take over users' accounts. These attacks are detected by analyzing the end user's true digital identity to identify anomalies and potential fraud.
- ThreatMetrix identified more than 100 million fraud attempts during this period. This represents an 80% growth over the previous year.

ATTACK VECTORS PER MONTH

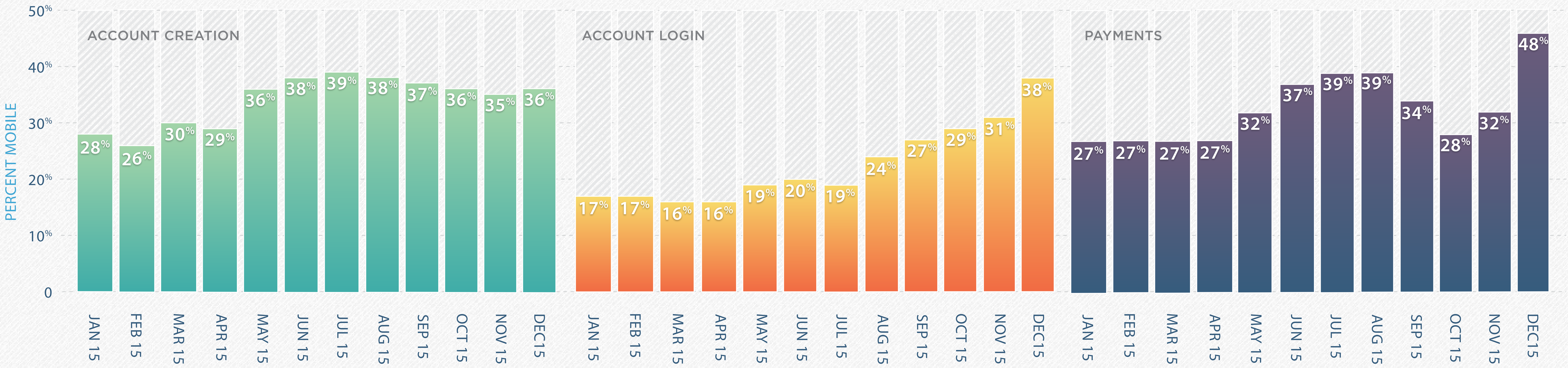


Note: The bar charts represent percentage of total transactions that were recognized at attacks

GROWTH OF MOBILE TRANSACTIONS

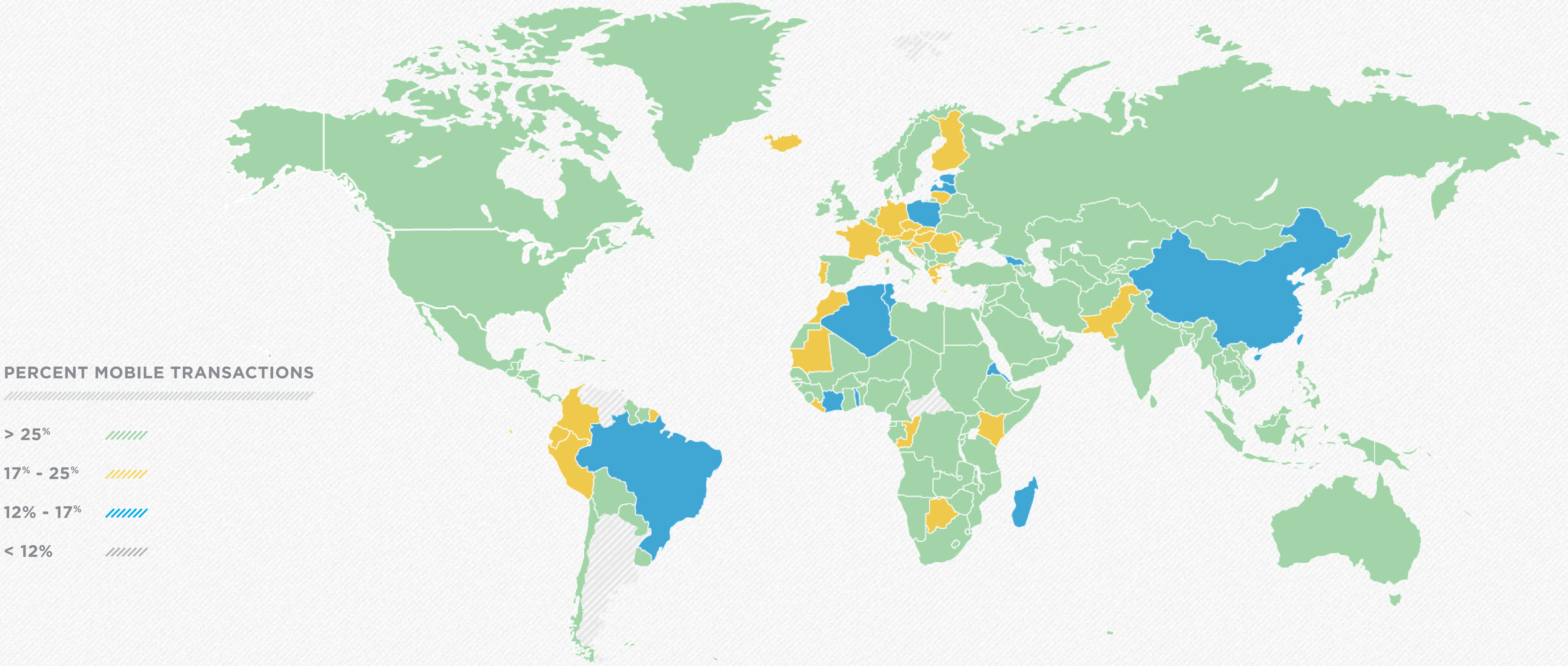
- The use of mobile to sign up, access or or pay for goods and services continues to grow for all industries and is a leading use case. This is represented in the continued increase in attacks using stolen identities and compromised devices, making application integrity, device security and identity verification far harder to control.
- Mobile transactions grew 200% compared to the previous year, primarily driven by the increase in account logins using mobile devices. This makes it critical for businesses to detect fraudsters while eliminating friction for trusted users.
- Shared intelligence and a multi-layered approach to identity proofing is crucial. ThreatMetrix Mobile delivers a complete set of digital intelligence around device identification, location services, malware detection, anomaly and device spoofing detection, jailbreak and root detection and application integrity evaluation.

PERCENT MOBILE PER TRANSACTION TYPE PER MONTH



MOBILE TRANSACTION PREVALENCE

Strongest mobile activity this quarter driven by high cross-border volumes during the peak holiday shopping days and China's Singles Day.



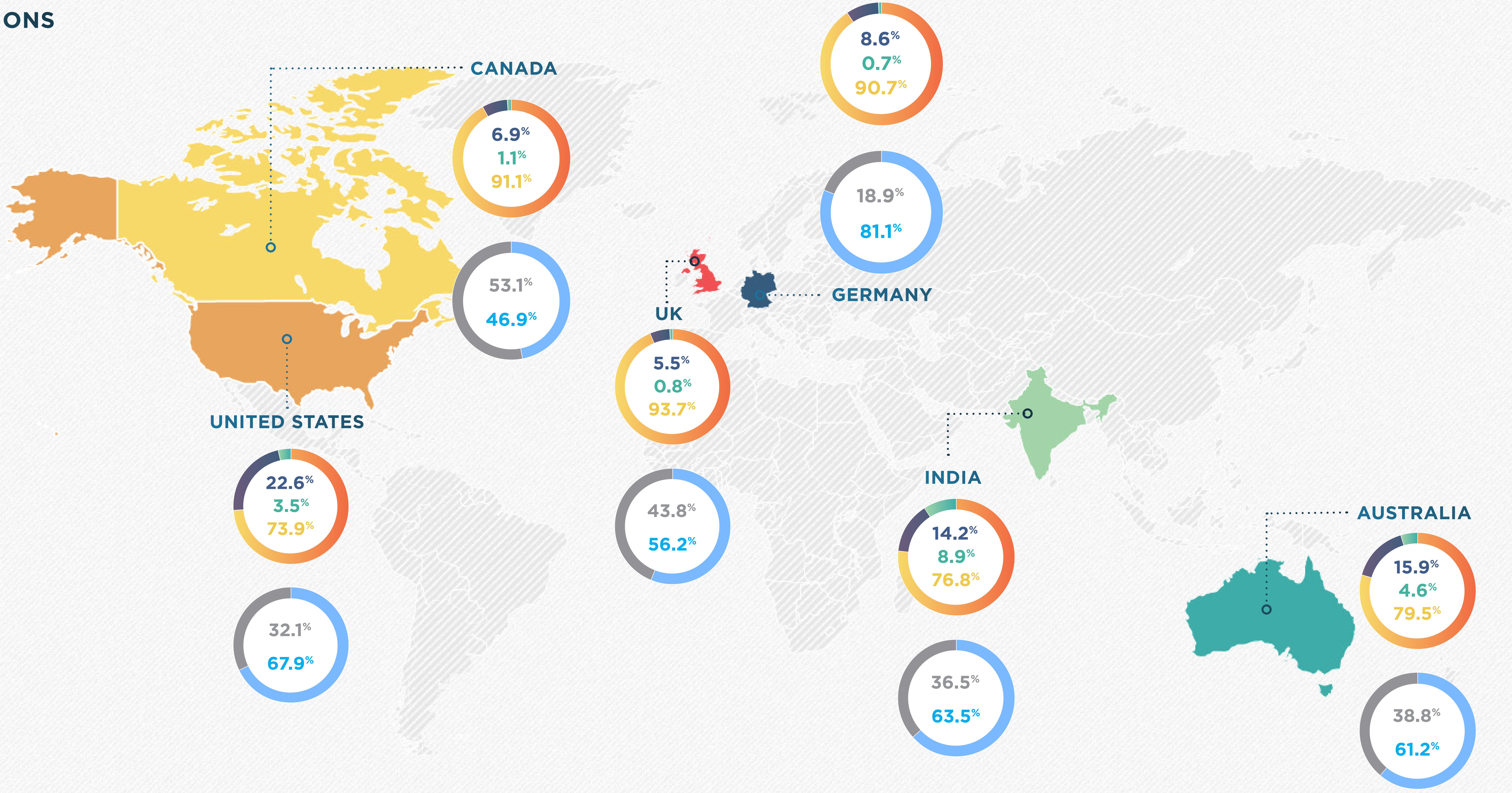
TOP MOBILE NATIONS

TRANSACTION TYPE

- ▨ PAYMENTS
- ▨ ACCOUNT CREATION
- ▨ ACCOUNT LOGIN

MOBILE

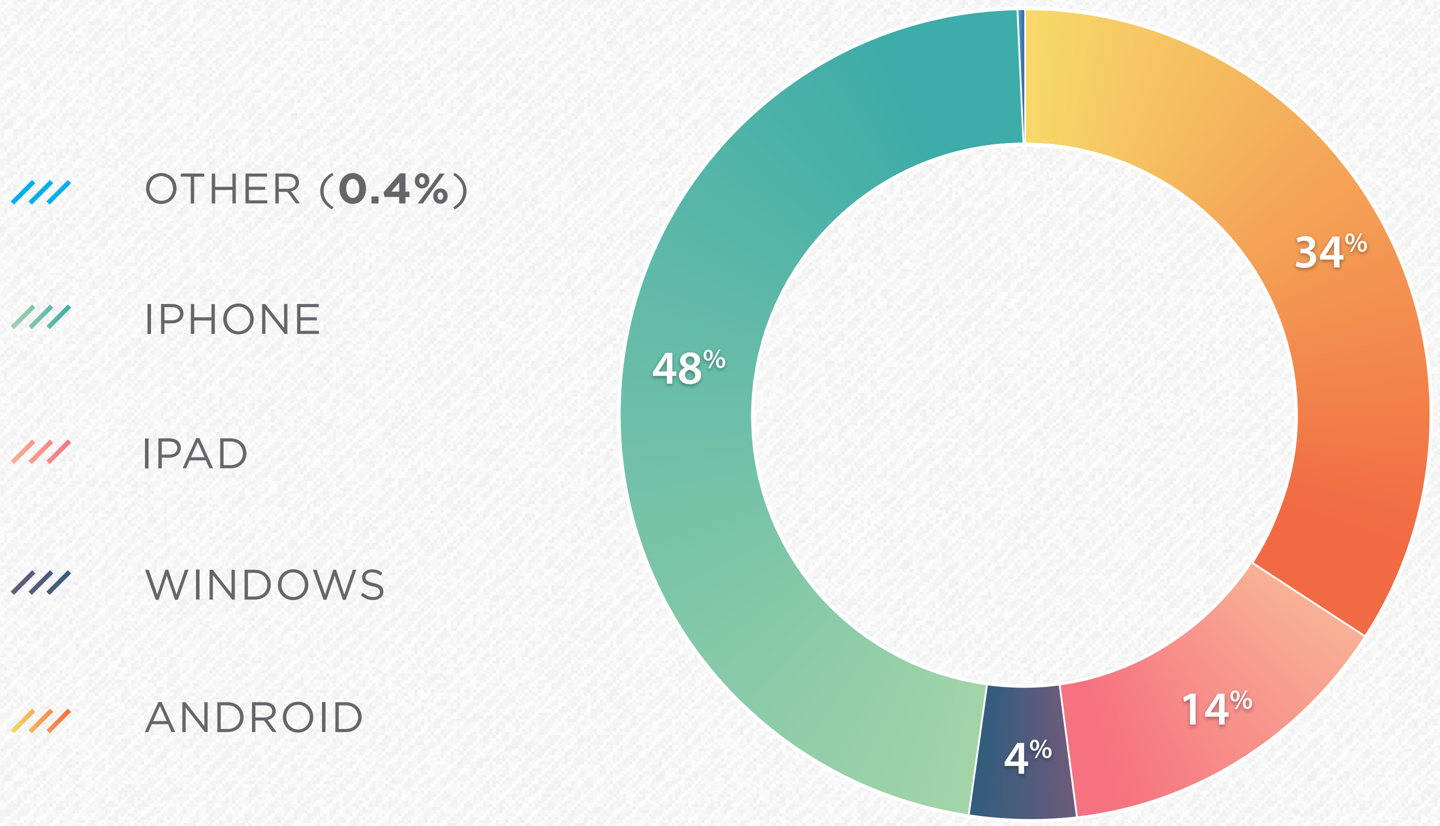
- ▨ MOBILE
- ▨ DESKTOP



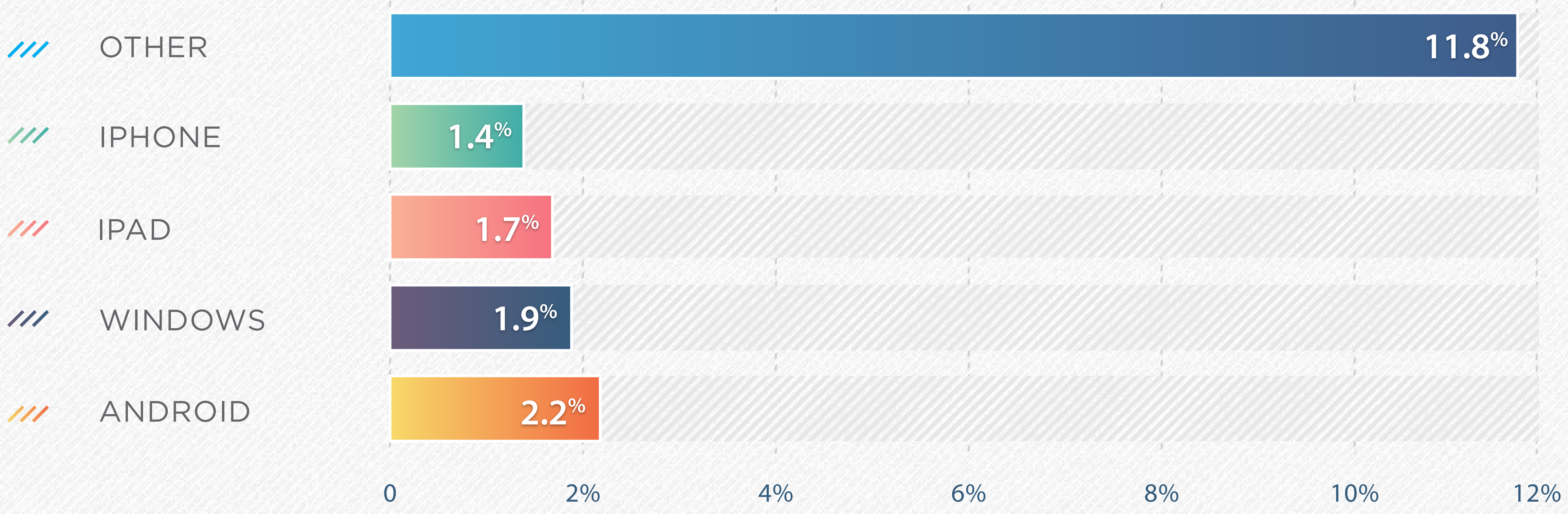
MOBILE TRANSACTIONS AND ATTACKS

- More than 350 million new mobile devices were added to the ThreatMetrix Digital Identity Network in 2015, primarily due to mobile application downloads as more and more consumers used mobile applications to shop and access banking sites and services.
- Attacks targeted at mobile devices and platforms are steadily growing. Spoofing, or fraudsters imperfectly impersonating a given mobile device (shown as "Other") constitute the most common source of these mobile attacks.
- iOS devices (iPhone and iPad) still account for the majority of total mobile transactions. iPhone's share of volume has increased by 60% compared to 2014.

VOLUME PER MOBILE OS / DEVICE

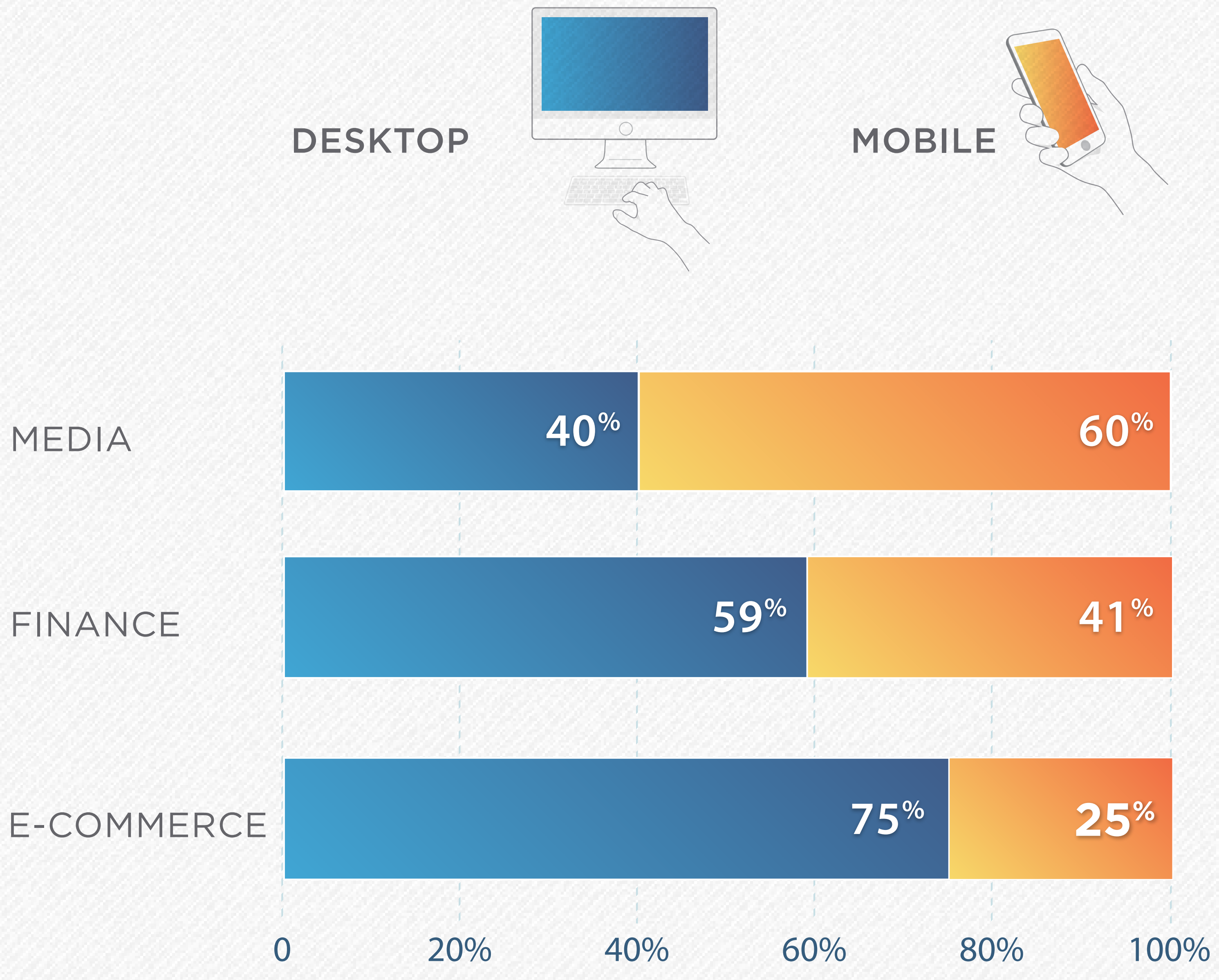


REJECT RATE PER MOBILE OS / DEVICE

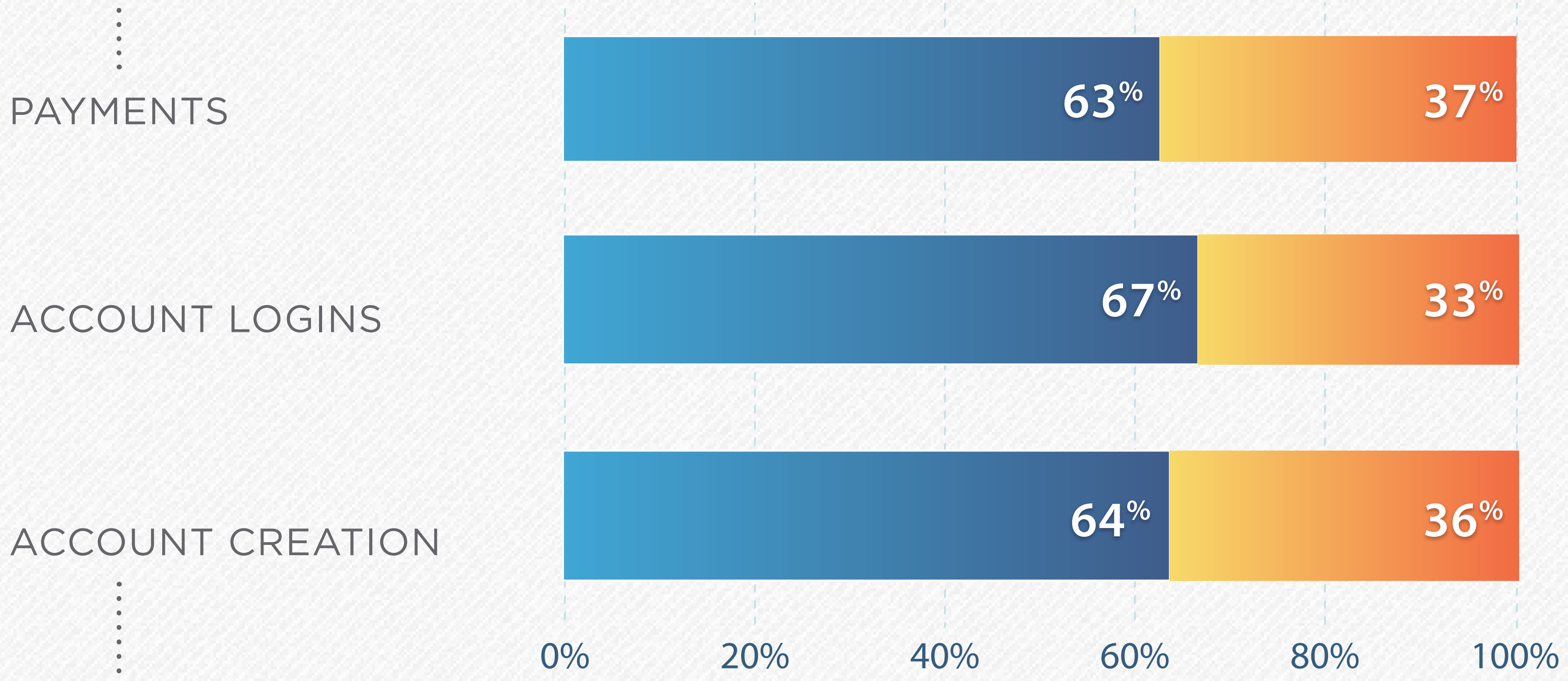


MOBILE VS. DESKTOP TRANSACTIONS AND ATTACKS

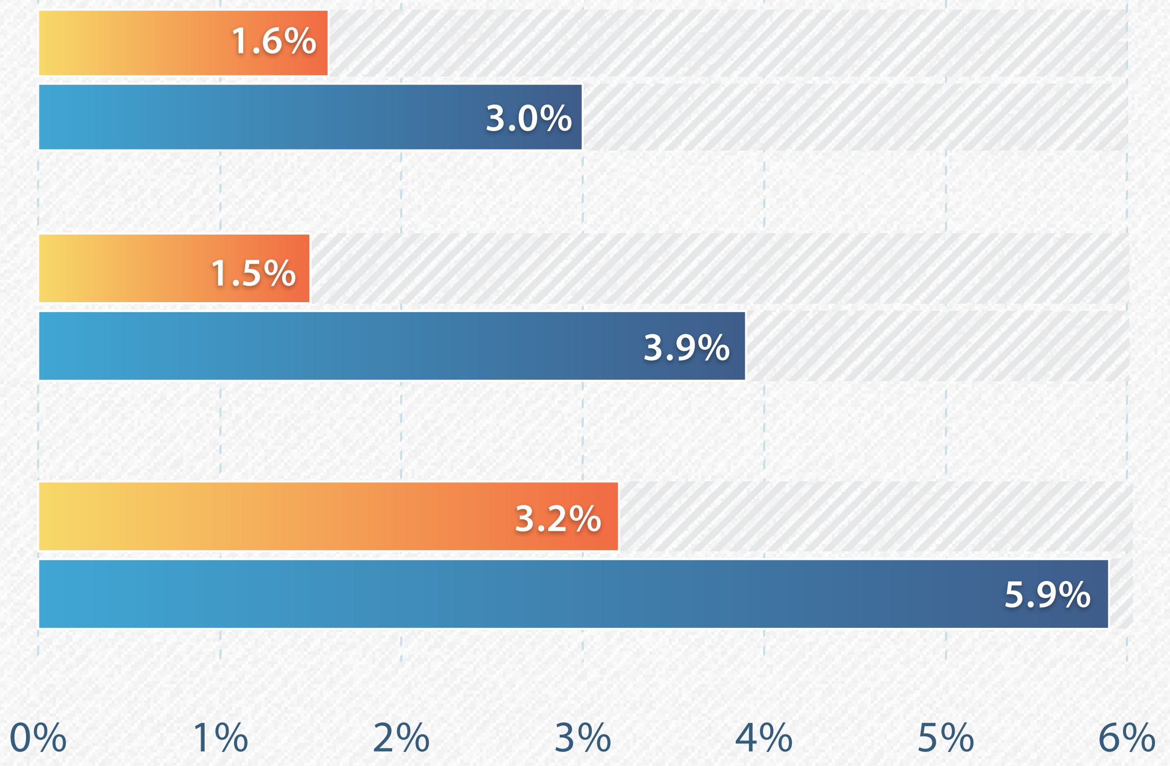
- Mobile-based commerce represented 34% of the total transactions analyzed. This represents a 200% growth in transactions originating from mobile devices compared to 2014.
- The biggest driver of this growth is coming from financial institutions whose share of mobile has steadily grown. This is driven by user adoption as well as deployment of digital solutions by the banks.
- The prevalence of stolen identities and tools to enable cloaking / spoofing is causing attacks targeted at mobile devices to continually increase.



VOLUME MOBILE VS DESKTOP



VOLUME MOBILE VS DESKTOP

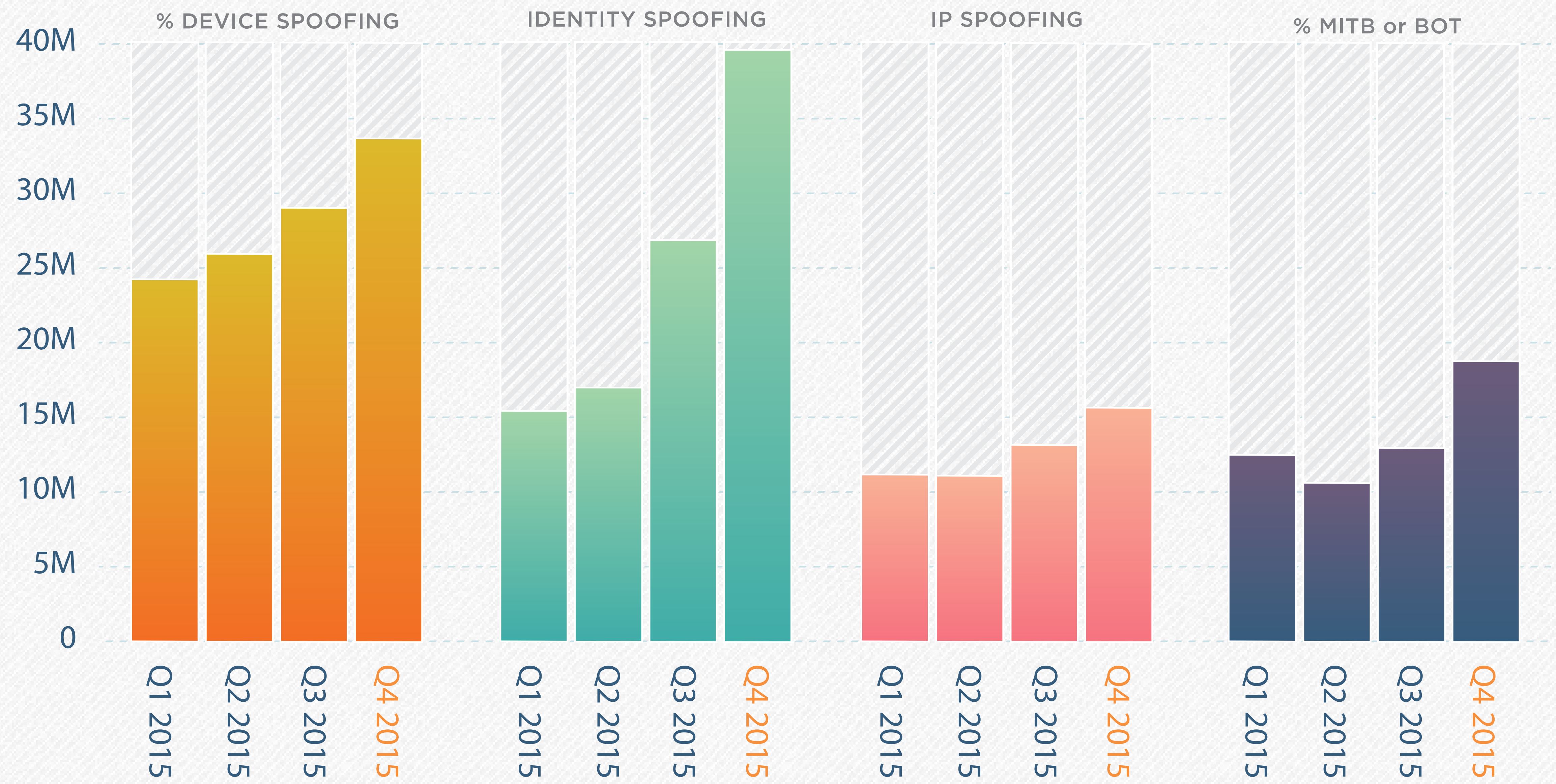


REJECT RATE MOBILE VS DESKTOP

MOBILE TRANSACTION AND ATTACK TRENDS

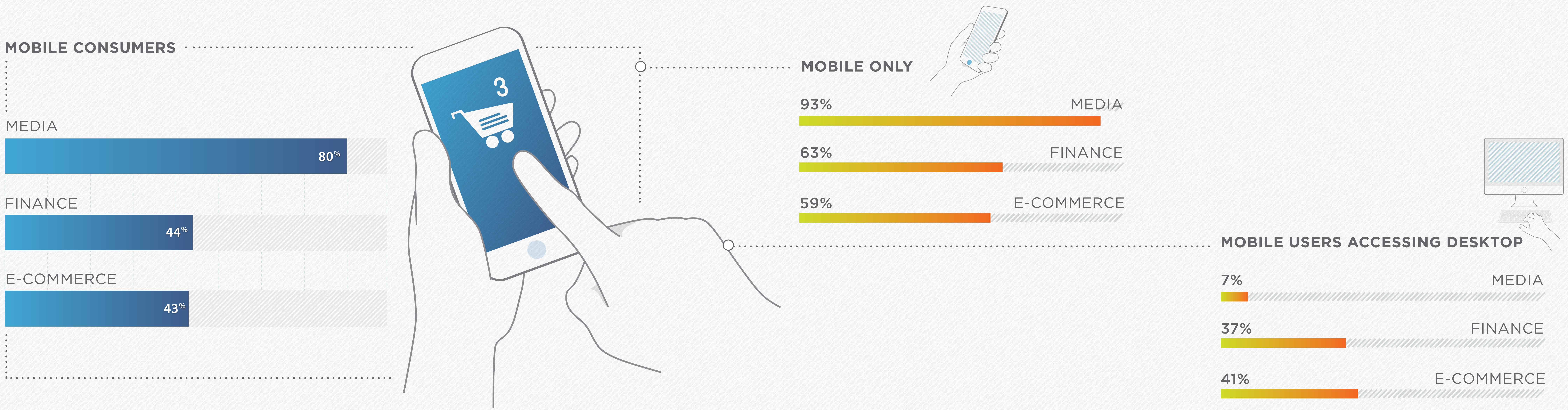
- As the transaction levels have gone up over the last year, so have the attacks.
- Key attack vectors that fraudsters are leveraging are:
  - Unsecured wireless networks to intercept user credentials.
  - Encouraging users to download hacked versions of legitimate applications from third party stores to deliver malware onto a device (which is generally jailbroken or rooted).
  - Intercepting personal information that can be inadvertently leaked by legitimate mobile applications.
- The number of attacks targeting connected devices grew significantly compared to the previous quarter. The biggest increase came from identity spoofing attacks which grew significantly compared to the previous quarter.
- The ThreatMetrix Digital Identity Network, coupled with powerful real-time decision analytics, allows the vast majority of mobile transactions and authentication attempts to be verified in real time against trusted patterns of behavior without adding friction to users or placing addition burden on business processes.

MOBILE ATTACK VECTORS



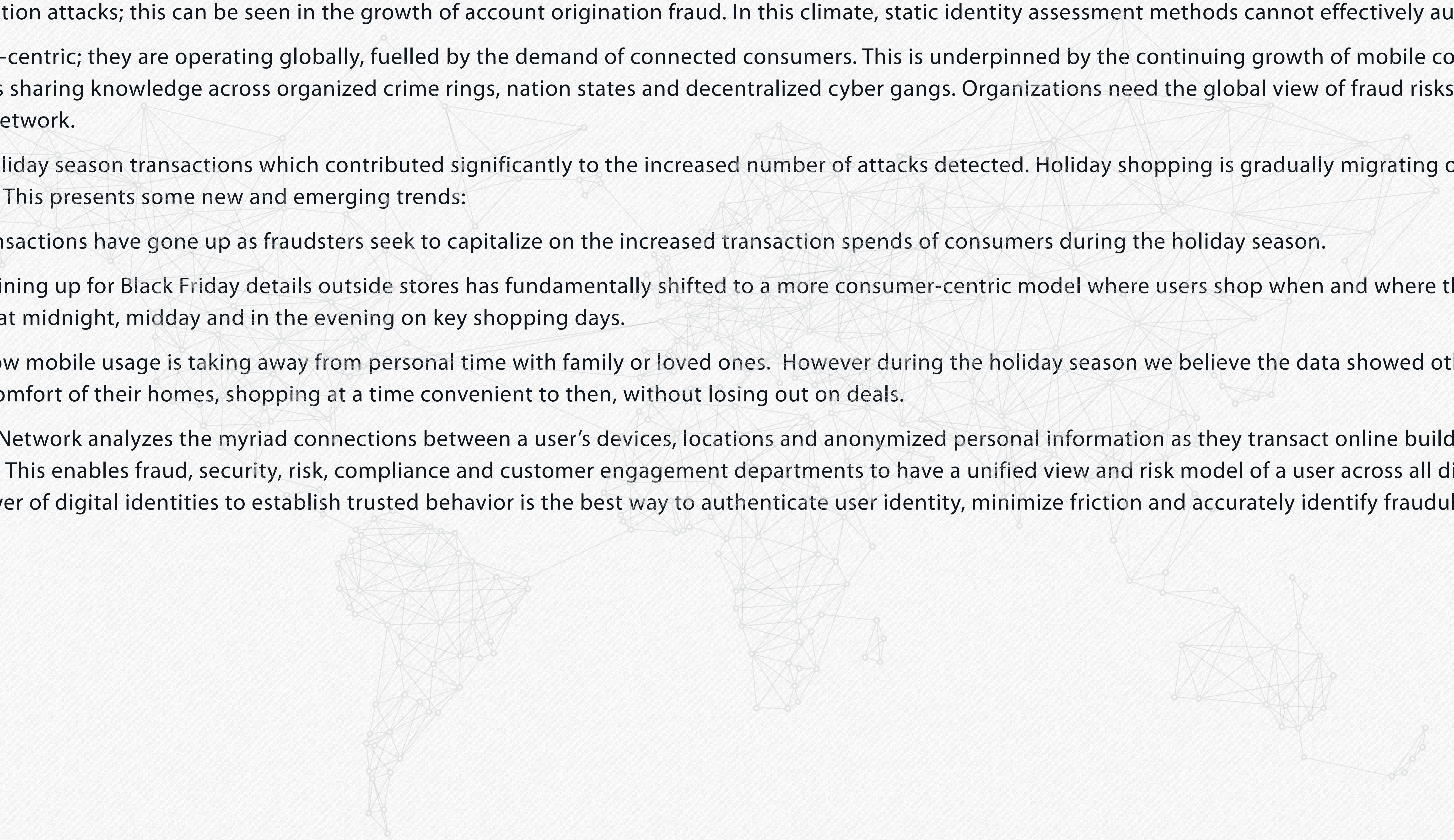
CROSS DEVICE USAGE

- More users accessed their bank account, made payments, streamed content and signed up for new accounts using their connected devices, moving seamlessly between devices.
- As consumers move between screens, they expect their experience to be consistent and frictionless. This requires a holistic recognition of trusted returning customers that looks beyond devices. Businesses need to evolve from a "mobile first" approach to a "digital first" approach.



CONCLUSIONS

- As this year concludes, cybercrime attacks continue to rise as fraudsters capitalize on easily available identity information following high-profile security breaches. Identity is a far more lucrative target for fraudsters than individual transaction attacks; this can be seen in the growth of account origination fraud. In this climate, static identity assessment methods cannot effectively authenticate user identity.
- Businesses are no longer location-centric; they are operating globally, fuelled by the demand of connected consumers. This is underpinned by the continuing growth of mobile commerce. Fraud attacks are following suit with cybercriminals sharing knowledge across organized crime rings, nation states and decentralized cyber gangs. Organizations need the global view of fraud risks that ThreatMetrix can provide via threat intelligence from The Network.
- This quarter saw a huge rise in holiday season transactions which contributed significantly to the increased number of attacks detected. Holiday shopping is gradually migrating online, with brick-and-mortar stores experiencing a fall in sales. This presents some new and emerging trends:
    - Basket values of rejected transactions have gone up as fraudsters seek to capitalize on the increased transaction spends of consumers during the holiday season.
    - The old trend of consumers lining up for Black Friday details outside stores has fundamentally shifted to a more consumer-centric model where users shop when and where they want. This was epitomized by digital transaction spikes at midnight, midday and in the evening on key shopping days.
    - There is a lot of talk about how mobile usage is taking away from personal time with family or loved ones. However during the holiday season we believe the data showed otherwise. Consumers were able to spend more time in the comfort of their homes, shopping at a time convenient to then, without losing out on deals.
- The ThreatMetrix Digital Identity Network analyzes the myriad connections between a user's devices, locations and anonymized personal information as they transact online builds a unique and trusted digital identity that fraudsters can't fake. This enables fraud, security, risk, compliance and customer engagement departments to have a unified view and risk model of a user across all digital channels and lifecycle and engagement. Leveraging the power of digital identities to establish trusted behavior is the best way to authenticate user identity, minimize friction and accurately identify fraudulent or high-risk behavior.



GLOSSARY: INDUSTRY TYPES

Financial Services

Includes mobile banking, online banking, online money transfer, lending, brokerage, alternative payments and credit card issuance.

E-Commerce

Includes retail, airlines, gambling, gaming, travel, marketplaces, ticketing and digital goods businesses.

Media

Includes social networks, content streaming and online dating sites.

GLOSSARY: 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.

Media

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

GLOSSARY: PERCENTAGES

Transaction Type Percentages

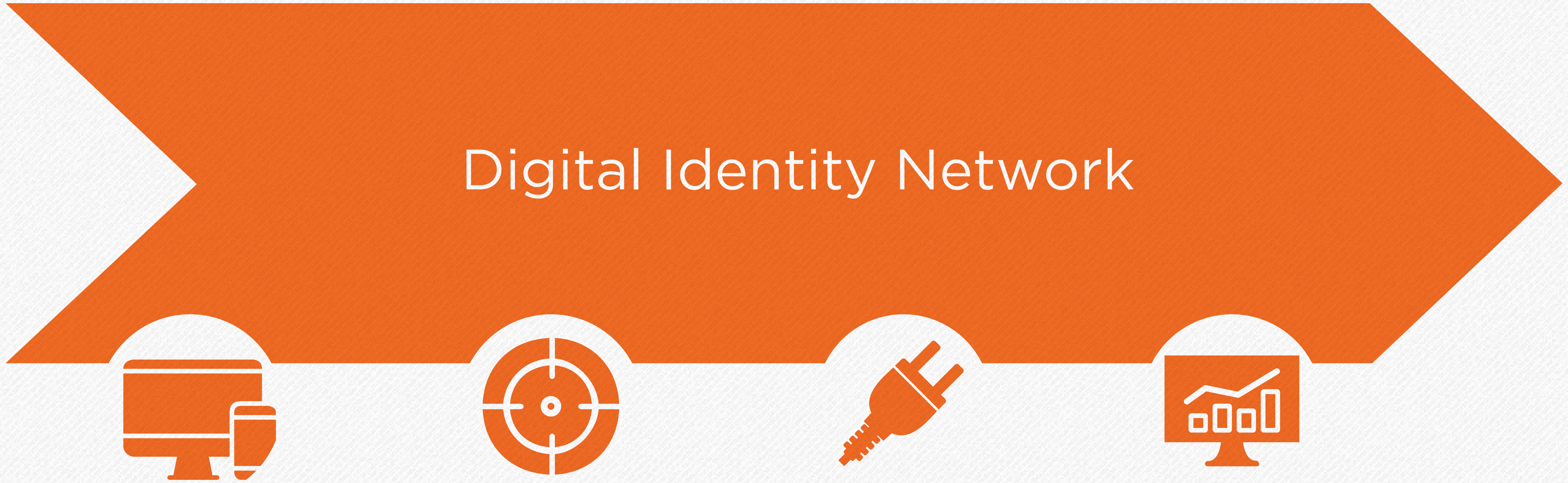
Are based on the number of transactions (account creation, account login and payments) from mobile devices and computers received and processed by the ThreatMetrix Digital Identity Network.

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.

GLOSSARY: THE THREATMETRIX DIGITAL IDENTITY NETWORK

The ThreatMetrix digital identity network leverages global shared intelligence across millions of daily consumer interactions including logins, payments and new account originations. An anonymized identity of each consumer is created combining specific device and persona detail that each individual used at any given time and at any place. Fraudulent activities are also captured in detail. Each new transaction is then analyzed in milliseconds through profiling of a users' device, identity, behavior and threats enabling companies transacting on the Internet to accurately and transparently authenticate users instantly without compromising user privacy.



Digital Intelligence

1. Mobile App SDK
2. Web SDK
3. End-Point & IOT SDK

Integration & Orchestration

1. Real-time APIs
2. Real-time Database
3. Integration Hub

Real-time Analytics

1. Business Rules
2. Behavior Analytics
3. Machine Learning

Decision Management

1. Search & Link Analysis
2. Reporting & Visualization
3. Case Management

GLOSSARY: 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 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 techniquesed user accounts or unusual identity linkages and usage.

IP Address Spoofing

Includes social networks, content streaming and online dating sites.

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.

THANKYOU

ThreatMetrix®

ThreatMetrix®, The Digital Identity Company, is the market-leading cloud solution for authenticating digital personas and transactions on the Internet. Verifying billions of annual transactions supporting tens of thousands of websites and thousands of customers globally through the ThreatMetrix® Digital Identity Network, ThreatMetrix secures businesses and end users against account takeover, payment fraud and fraudulent account registrations resulting from malware and data breaches. Key benefits include an improved customer experience, reduced friction, revenue gain, and lower fraud and operational costs. The ThreatMetrix solution is deployed across a variety of industries, including financial services, e-commerce, payments and lending, media, government, and insurance.

Cover image by Everything Possible

BACK TO START