ThreatMetrix®
Cybercrime Report: Q1 2015

The TheatMetrix Cybercrime Report examines actual cybercrime attacks detected and analyzed by the ThreatMetrix Digital Identity Network during Q4 2014 and Q1 2015.

ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

Foreword

I spend a lot of time talking to our customers. Standing alone they were drowning under wave after wave of bot attacks, data breaches and fraud losses, but combined they have been able to turn the tide on their attackers. Our Cybercrime Reports are intended to help educate and provide valuable insight into cyber threat and fraud trends that otherwise lurk beneath the surface and hide among, and hurt, your legitimate customers.

With the world's largest digital identity network, built on the shared intelligence from over a billion transactions per month from some of the world's largest businesses, ThreatMetrix is in a unique position to monitor and analyze the key trends that are shaping the new age of connected commerce. During the 2014 holiday season, we saw record transaction volume across mobile and Web. These transactions further showcased that online/mobile commerce is the biggest emerging opportunity and risk for businesses trying to deliver frictionless experiences to their trusted customers without falling victim to the cybercriminals.

Consumers are increasingly getting comfortable with using their connected devices to access content, conduct commercial activities and make purchases. As expected, online retailers reported strong volumes but consumer activity was significant across all industries as they streamed more content, bought more tickets and checked their account balances more often, more than 25% of the time using their mobile devices.

This battle between the 'good guys' and the cybercriminals will continue to intensify with consumer personally identifiable information data in the wild. At ThreatMetrix, we strongly believe that it takes a network to fight the sophisticated network of cybercriminals. Shared intelligence is the key to protect against the "digital debris" that comes from data breach fallouts.

Alisdair Faulkner
Chief Products Officer
ThreatMetrix

Report Overview

The Q1 ThreatMetrix Cybercrime Report is based on actual cybercrime attacks from the October 2014 –March 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 registrations.

- The Network analyzes more than one billion transactions per month, nearly a third 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 users benefit from a global view of risks, based on these attributes and rules specifically custom-tuned for their business.
- Attacks discussed are from "high risk" transactions scored by ThreatMetrix.

Q1 2015 Cybercrime Report – Key Highlights

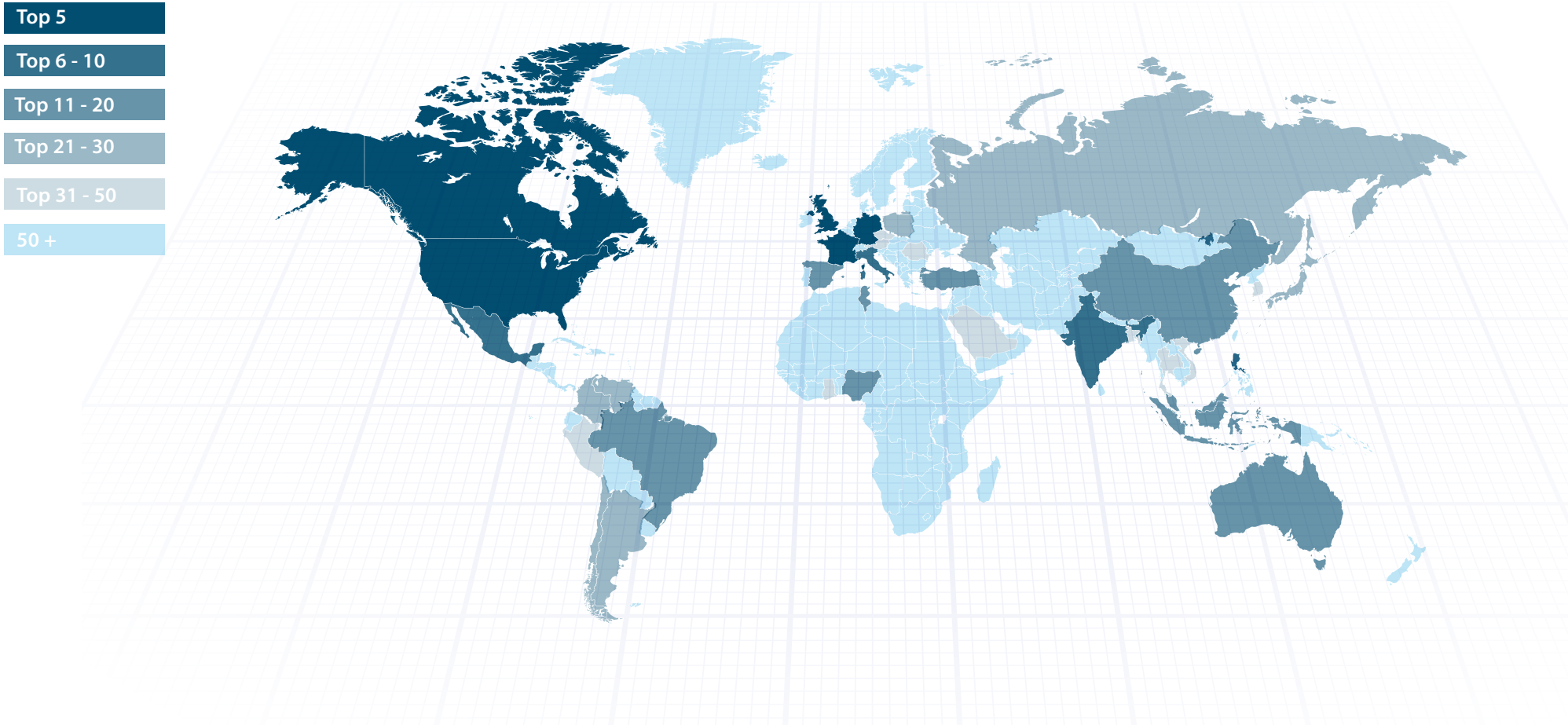
2014 holiday season was a period of record online transactions: "Cyber Monday" online sales exceeded $2B for the first time with a significant portion coming from mobile devices.

Through its analysis of the top customer transactions across industries, Threatmetrix highlights the following representative key market trends:

- Trust is critical for conversion and customer loyalty. 74% of holiday transactions originated from existing accounts as consumers returned to their favorite merchants.
- Impersonation or "spoofing" attacks continue to rise driven by the billions of breached identities in the wild and the prevalence of crimeware tools. ThreatMetrix identified more than 11.4 million fraud attempts during peak holiday shopping periods.
- Mobile usage continues to grow, accounting for up to 31% of transactions. With more than 20 million new mobile devices being added to The Network every month, this trend is expected to continue.
- More Android devices were identified this period compared to before. We expect this trend to continue as emerging markets increasingly do business via more affordable Android devices. Despite more Android devices being added, iOS devices accounted for two-thirds of mobile transactions.

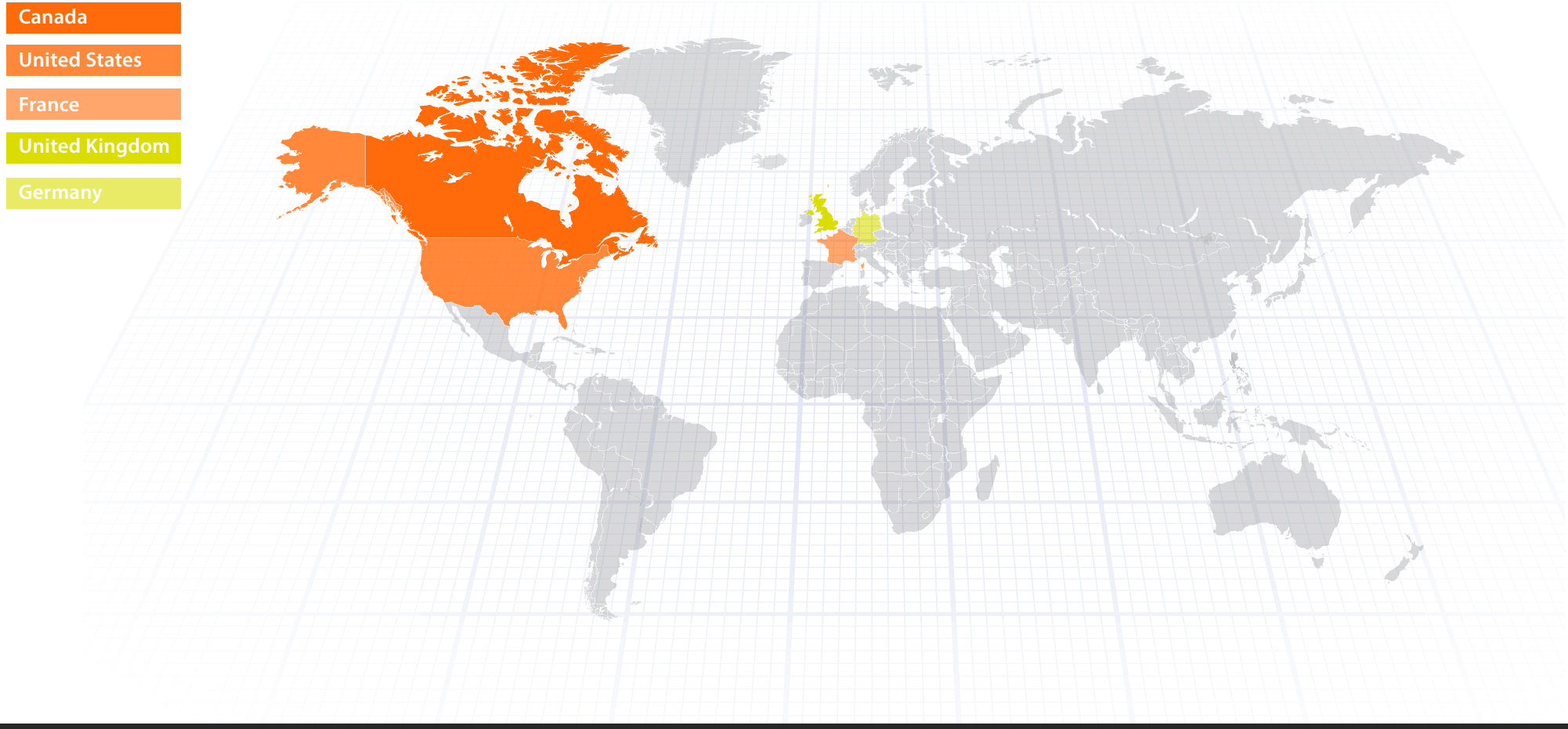
Attack Origins by Geography: Total number of attacks detected by geography of origin

- Cybercrime is a global phenomenon with fraudsters targeting businesses across countries.
- Despite the global nature of cybercrime, the majority of attacks originate in the countries with high online and mobile volume.



Top attack origins by Geographies

The majority of attacks originated from and targeted the same country. Top 5 attack originations and target countries were:



Transaction Analyzed by Industries

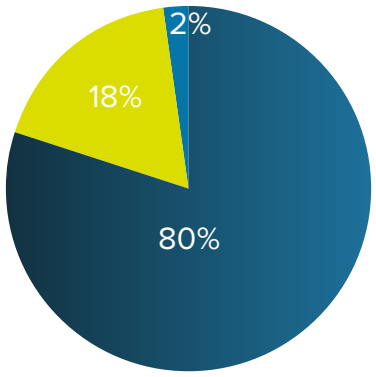
ThreatMetrix transactions span e-commerce, financial services, and media sectors. While login and new account creations are the primary use cases for Financial Services and Media, payment transactions are the dominant use case for the e-commerce sector.

Payment transactions and login transactions grew significantly during this period as consumers revisited retailers to view offerings/deals and make their holiday purchases.

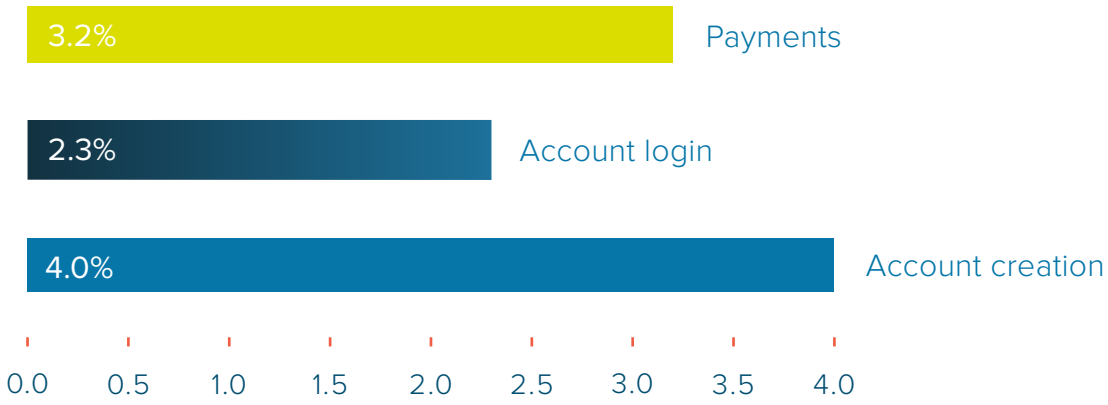
ThreatMetrix is deployed on 10 of the top 20 e-commerce merchants in the U.S.

While new account creation rates were lower than other transaction types, their share of fraudulent transactions rose, driven by the stolen identities made available to the cybercriminals following massive breaches.

Volume by Transaction Types



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.

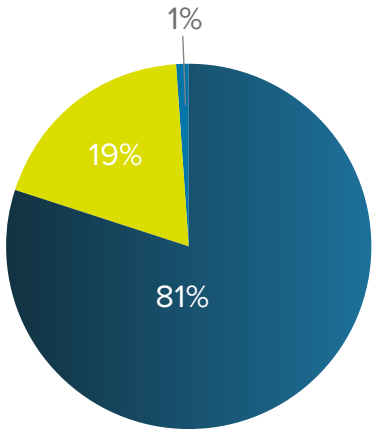
E-Commerce Transactions and Attacks

During the peak holiday shopping season, customers overwhelmingly went to the sites they trust to either shop for goods or browse for deals.

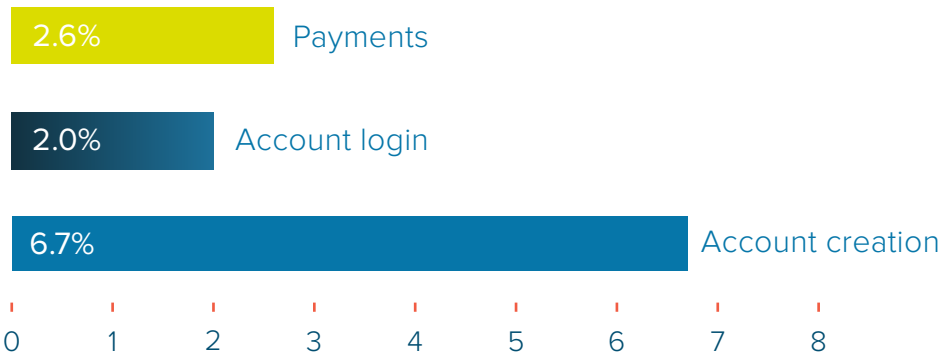
- Consumers typically store their payment information on file with 3-4 of their favorite/trusted merchants and have to log-in to their accounts to make purchase/save items for future purchase.
- As a result, account logins were a much larger portion of total transactions, during this period with customers revisiting their shopping carts to complete purchases.
- A significant portion of multi-device consumers move sequentially between several screens for everyday activities like booking a hotel or shopping for electronics. The Network is able to track and provide intelligence across these devices to identify trusted consumers.

New account creations were significantly lower but represented the highest percentage of attacks as fraudsters increasingly used account creation as a means to make purchases using stolen credentials.

Transactions by Type



Attacks by Transaction Type



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

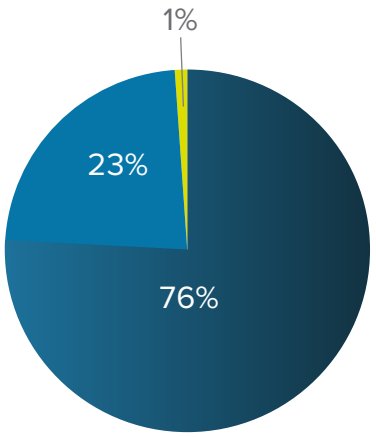
Financial Services Transactions and Attacks

While online banking authentication transactions continue to dominate the financial services industry, the payment transactions increased during this period, driven by the increasing consumer adoption, use of alternate payment instruments and banking card authentication solutions, and increase in online gifting during the holiday season.

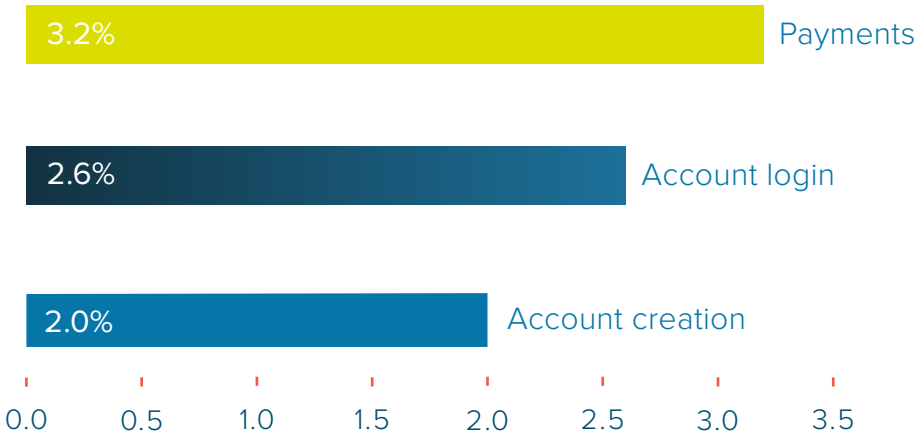
In Financial Services transactions, the impact of consumer credentials made available by data breaches, was evidenced by a substantial increase in fraud rates across all transaction types.

The prevalence of crimeware tools was also evidenced by the increase in the payment and login frauds over the previous period.

Transactions by Type



Attacks by Transaction Type



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

Media Transactions and Attacks

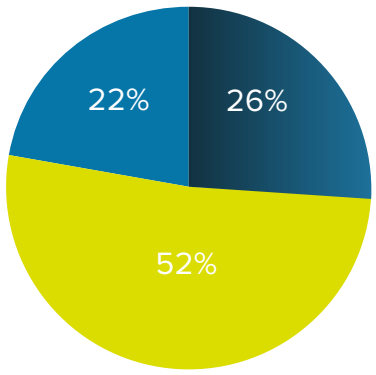
ThreatMetrix's analysis demonstrates a strong growth in payment transactions through media organization and a higher than average fraud levels compared to other industries.

The large number of data breaches reported by US companies has led to hundreds of millions user credentials increasingly being used on media sites for criminal intent. Modest sign-up and authentication requirements along with user password sharing across sites continue to attract the highest rate of cybercrime attacks per transaction.

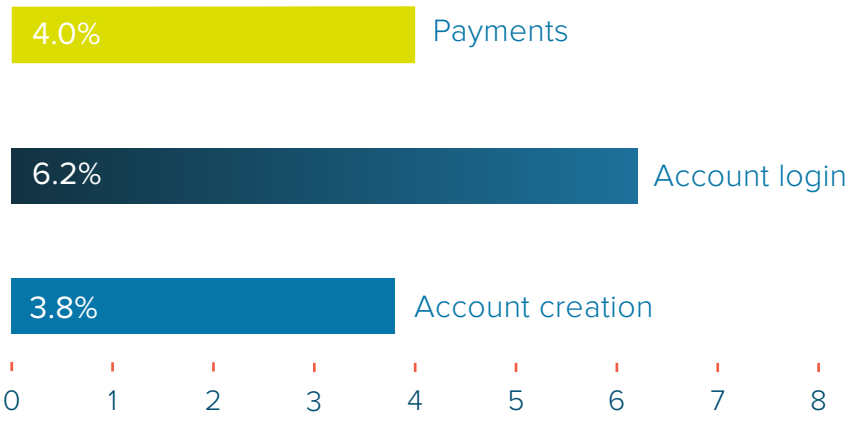
The Network saw a strong growth in payment transactions through Media organizations and higher than average fraud levels when compared to other industries.

Illegal access to content outside of approved geographies, combined with spamming, and fraudulent bot-driven account creation, represent the key drivers of fraudulent transactions in the Media space.

Transactions by Type



Attacks by Transaction Type



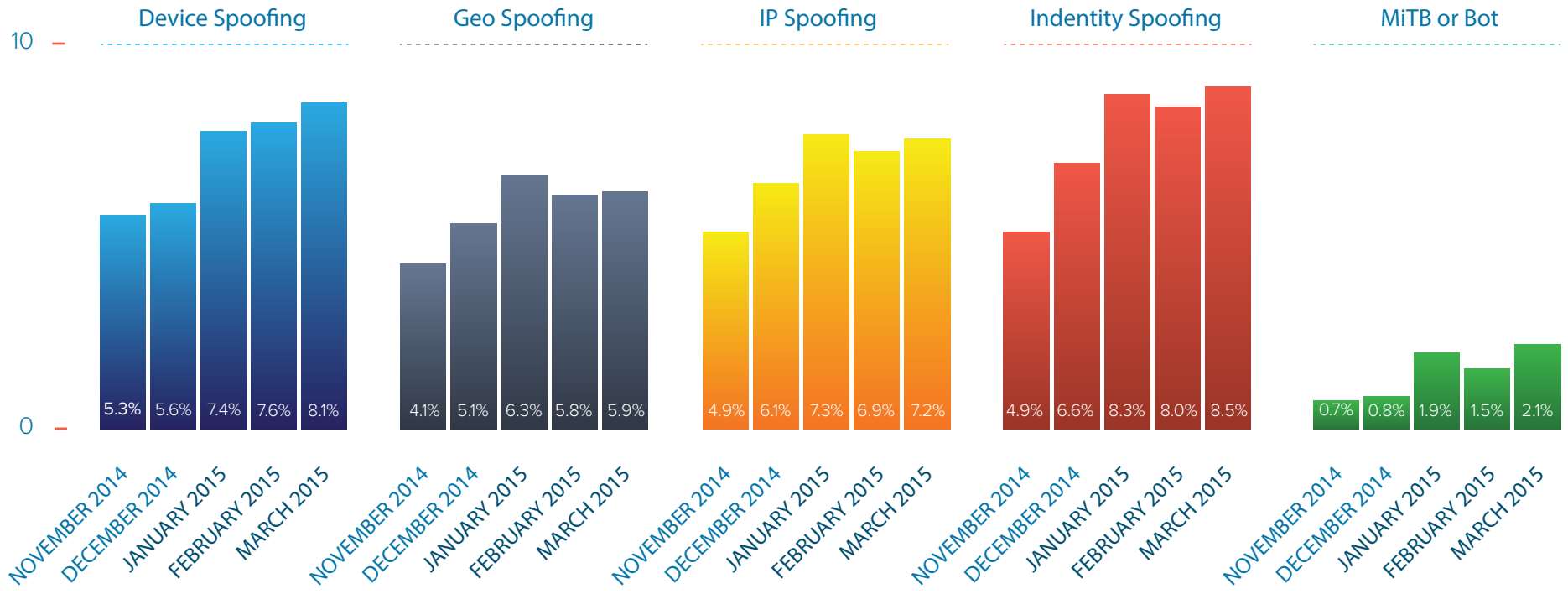
Media includes social networks, content streaming and online dating sites.

Top Attack Vectors

Impersonation or "spoofing" attacks continue to rise driven by the availability of more sophisticated device spoofing tools combined with hacked and breached identities. These crimeware tools target businesses that are using first generation browser fingerprinting technology.

ThreatMetrix platform is built from the ground up to evaluate the normality and anomalies of the browser characteristics that these tools will exploit. This is done by fingerprinting the device at multiple layers to reveal inconsistencies, and detect spoofing.

ThreatMetrix identified more than 11.4 million fraud attempts during peak holiday shopping (Nov –Dec 2014).



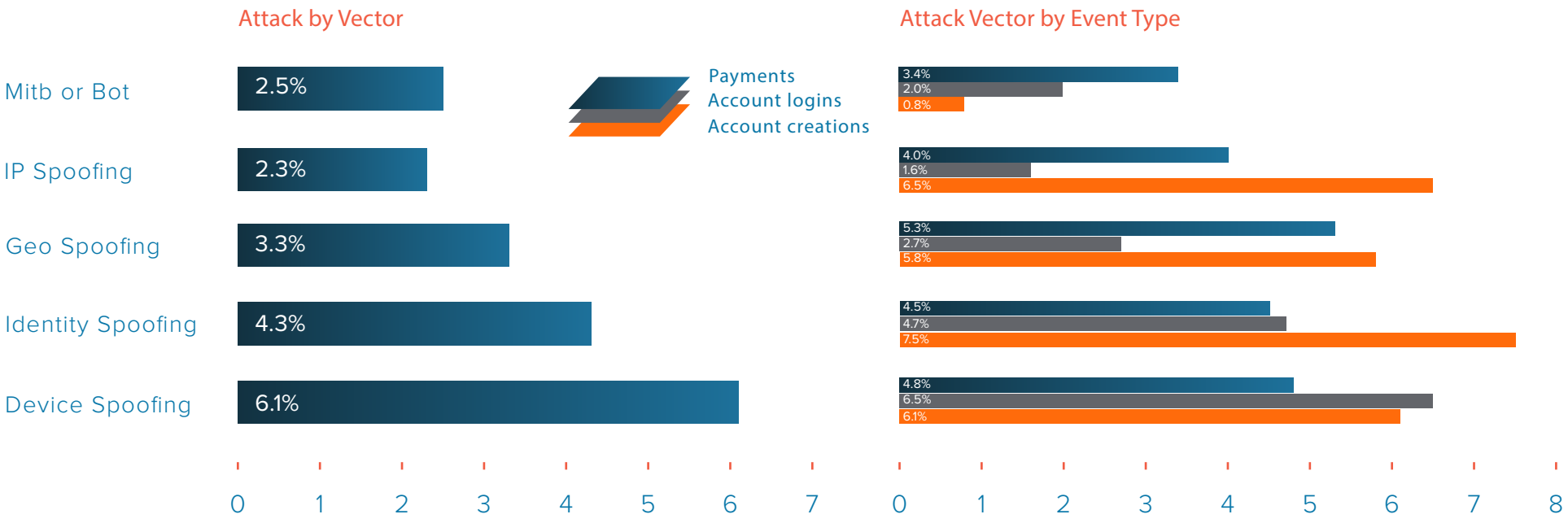
ThreatMetrix® BUILDING TRUST ON THE INTERNET™

Top Attack Methods

Attack vectors are analyzed in real time by the Network's global policies.

Some attacks use multiple vectors, but device spoofing remains the top attack vector, with more than six percent of transactions.

As crimeware tools gain traction, increasing cloaked traffic is evidenced in ThreatMetrix's network analysis, specifically for new account creation wherein the fraudsters use stolen identities along with these tools to defraud businesses.



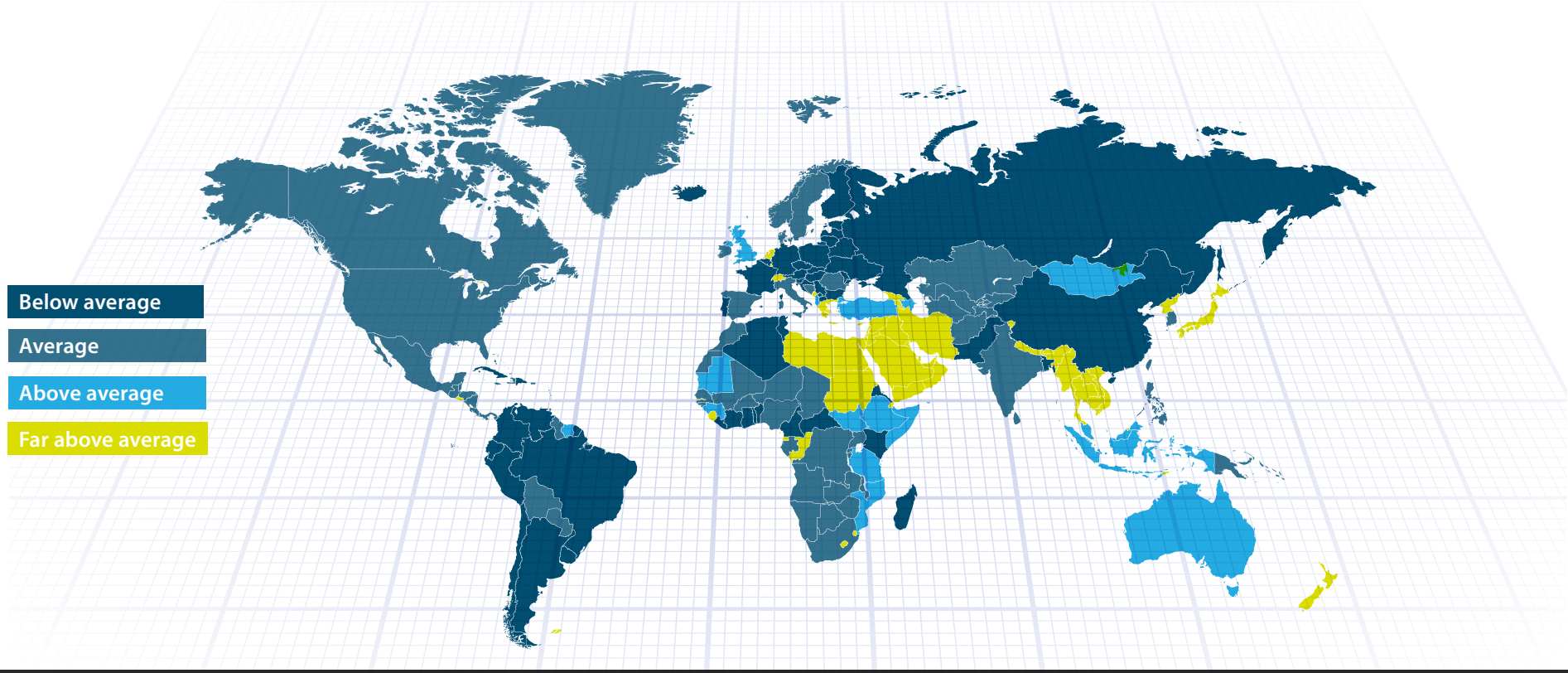
The bar charts represent percentage of total transactions that were recognized at attacks

Mobile Transaction Prevalences

Emerging markets are showing a rapid uptake of mobile phone ownership and usage of mobile services.

While mobile is a vehicle to drive financial inclusion for unbanked consumers, mobile transactions will be active targets for fraudsters.

- The network analyzes mobile transactions from over 200 countries and territories across the globe. Consumers from emerging economies conduct a much higher percentage of transactions using mobile devices.
- Customers in the U.S, Canada and Western Europe use both channels equally, while countries in the Middle East, Africa and Southeast Asia, among others, have a much higher share of mobile transactions.



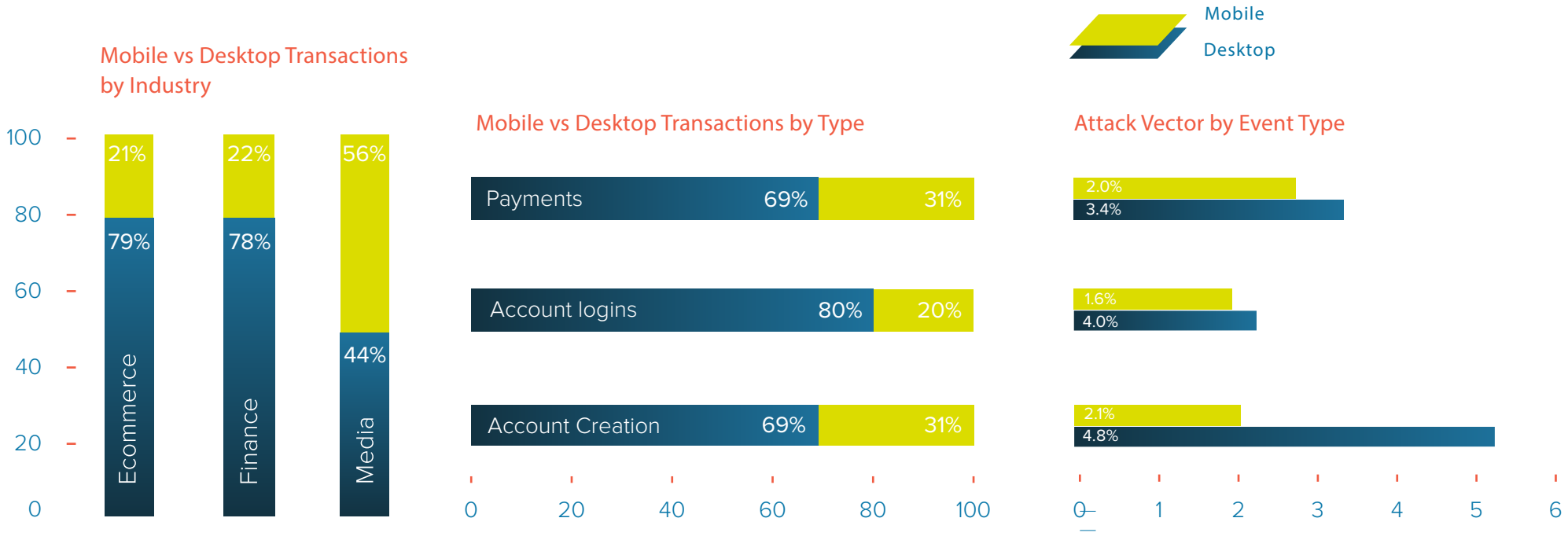
Mobile vs. Desktop Transactions and Attacks

Mobile device-based commerce represented nearly one third of the total analyzed. This number continues to grow across industries and transaction types.

Mobile usage represented the largest usage percentage for media channel as users increasingly accessed content/services on the go.

Mobile attacks continue to grow, driven by the prevalence of stolen identities and tools to enable cloaking/spoofing, but remain below the desktop volumes, as mobile devices are not yet conducive to massive fraud attacks.

New account creation using mobile devices is increasing but has lower instances of attack compared to desktop.



Mobile Transactions and Attacks

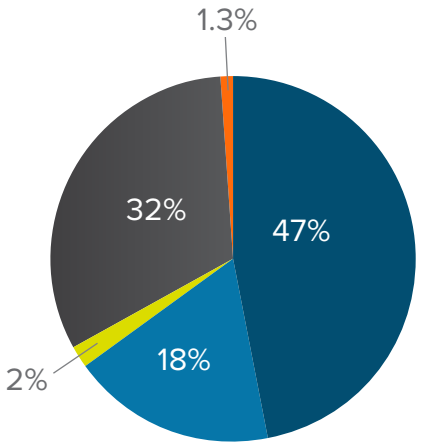
As mobile transactions are growing, so are the attacks targeted towards mobile devices and platforms. Spoofing or cybercriminals imperfectly impersonating a given mobile device (shown as "Other") constitute the most common source of these mobile attacks. ThreatMetrix's layered approach effectively detected and stopped these fraudulent transactions from devices masking their operating system (OS).

iOS devices (iPhone and iPad) combined accounted for nearly two-thirds of total holiday transactions. Android showed strong growth driven by customer deployment, launch of ThreatMetrix mobile SDK for Android and high Android growth rates especially in emerging market.

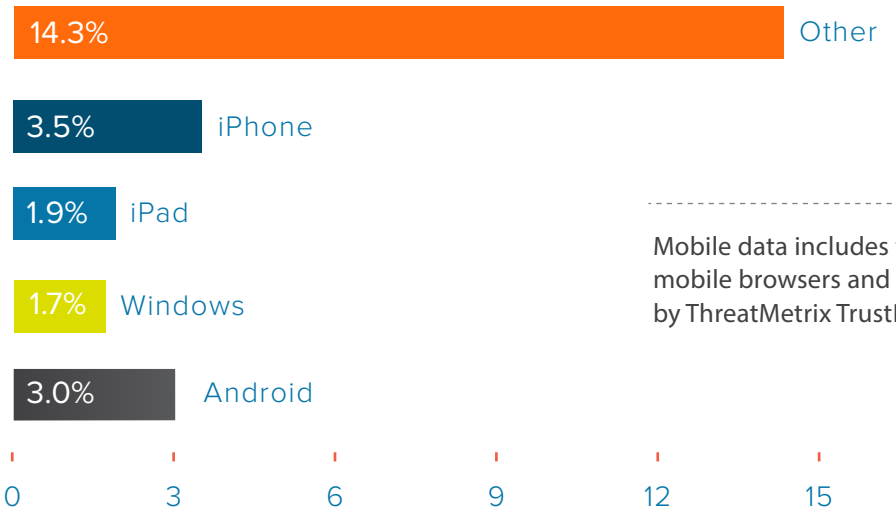
Despite Android's dominance in market and browser share, iOS generates nearly twice the number of payments, logins, and authentications of the other mobile operating systems combined.

iOS transactions data highlights that convenience still trumps form factor, with iPad usage being larger than iPhone even though iPhone ownership is far more common.

Volume per Mobile OS / Device



Attack per Mobile OS / Device

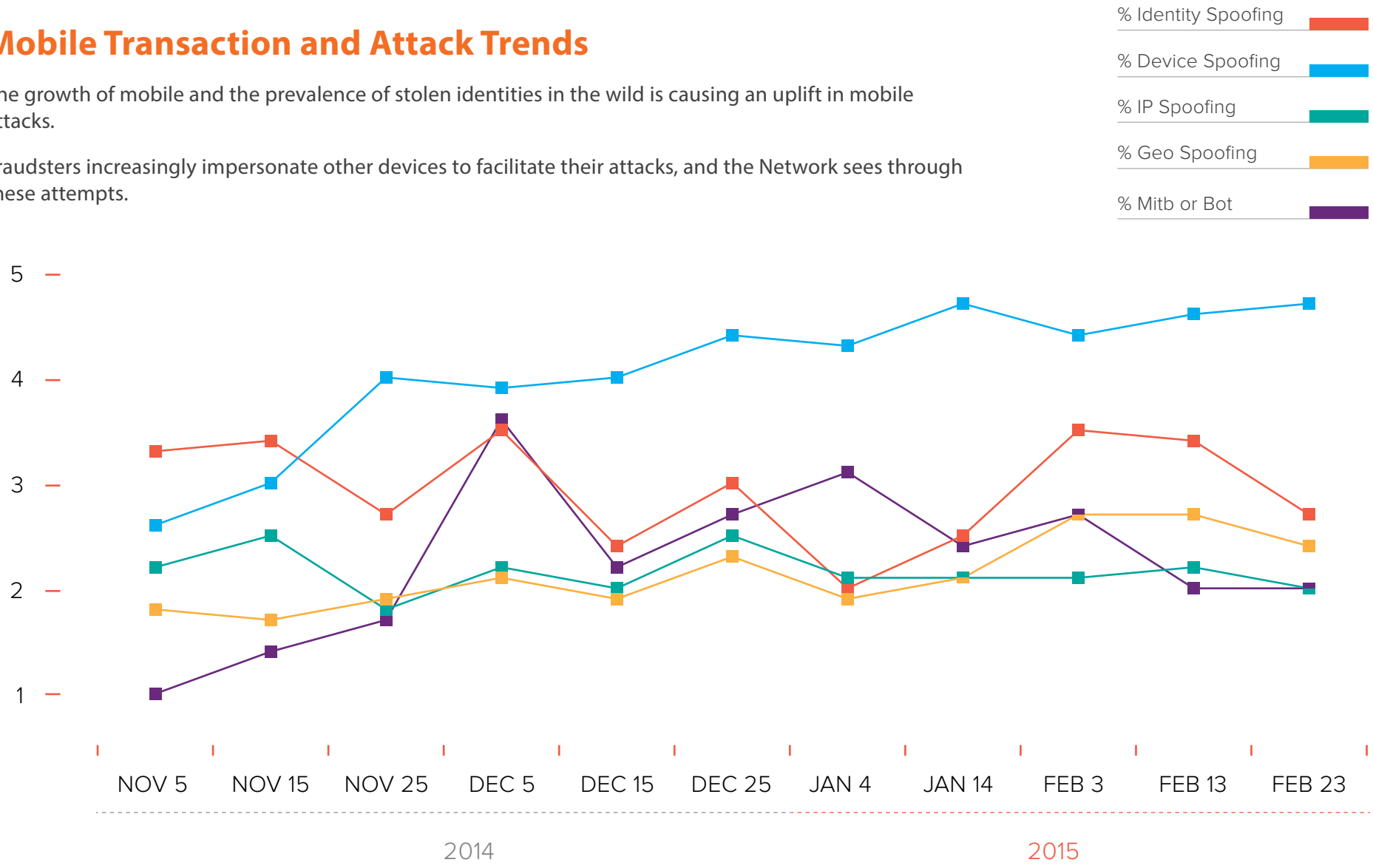


Mobile data includes transactions from both mobile browsers and mobile apps protected by ThreatMetrix TrustDefenderTM Mobile.

Mobile Transaction and Attack Trends

The growth of mobile and the prevalence of stolen identities in the wild is causing an uplift in mobile attacks.

Fraudsters increasingly impersonate other devices to facilitate their attacks, and the Network sees through these attempts.

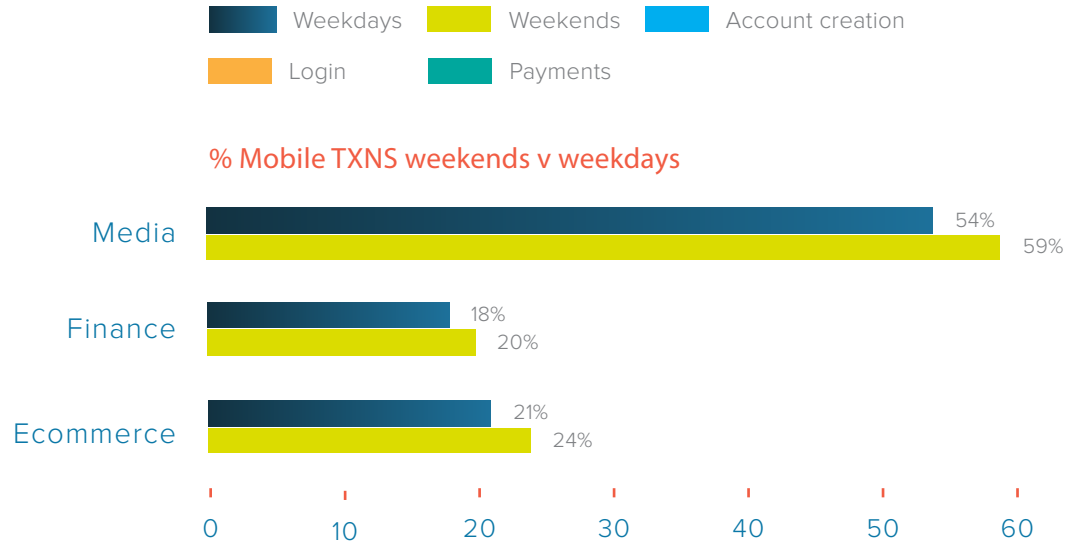


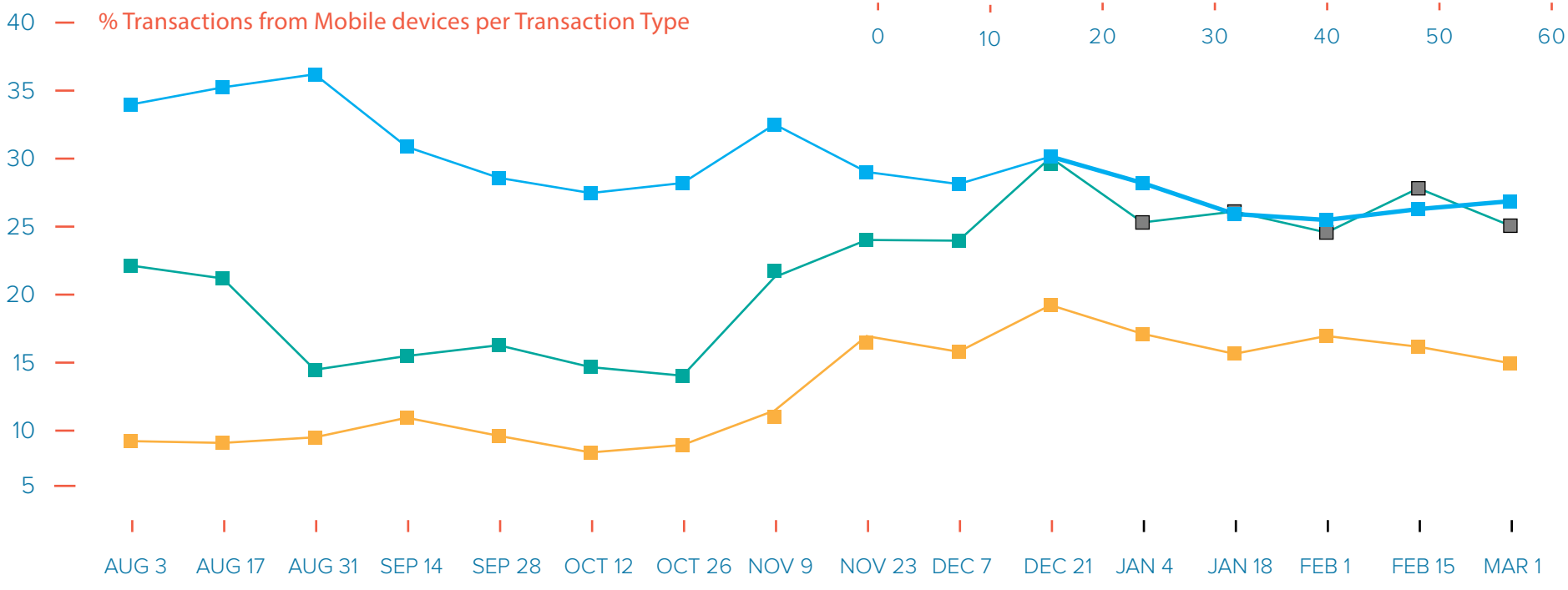
Mobile Transaction Trends

The usage of Mobile continues to grow as more and more customers switch to mobile to access content, conduct commerce transactions and buy product and services.

Mobile usage over the weekend is higher across industries as users increasingly rely on their connected devices.

Using mobile devices to sign up for services continues to be a leading use case. This makes it critical for businesses to eliminate friction for trusted users while stopping fraudsters.





ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

Conclusion

It is evident that the payment and commerce landscape is rapidly evolving due to the digitization of consumers and merchants, proliferation of connected devices, rise in alternative payments and growth of social media. Online and mobile commerce growth continues to outpace offline (brick and mortar) as connected devices are fast becoming the leading way for users to access commerce and banking services. Mobile is the biggest emerging opportunity and risk for businesses and financial institutions trying to deliver frictionless experiences to their customers.

As the businesses have evolved, so have Cybercriminals. This analysis confirms that Cybercrime continues to be a well-funded, organized business with sophisticated technology and strong knowledge sharing across organized crime rings, nation states and decentralized cyber gangs. Recent massive credit card and identity data breaches along with the growing sophistication of cybercriminals has resulted in an increase in attacks targeted toward businesses across all regions and industries.

Cybercriminals continue to share information as well as develop tools that will help bypass the first generation fraud prevention solutions that rely on browser fingerprinting. This makes shared global intelligence a critical tool to fight crime.

ThreatMetrix protects its customers and speeds the flow of business by quickly distinguishing trusted customers from cybercriminals. ThreatMetrix delivers advanced fraud protection, frictionless authentication, and customer protection through a real-time collective response using intelligence gathered from billions of transactions in the ThreatMetrix Network.

Glossary: Industry Types

Financial Services includes mobile banking, online banking, online money transfer, lending, brokerage 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.

Payments Fraud: 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 event types (account creation, account login and payments) from mobile devices and computers received and processed by the ThreatMetrix Global Threat Intelligence Network.

Attack Percentages are based on event types 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: 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.

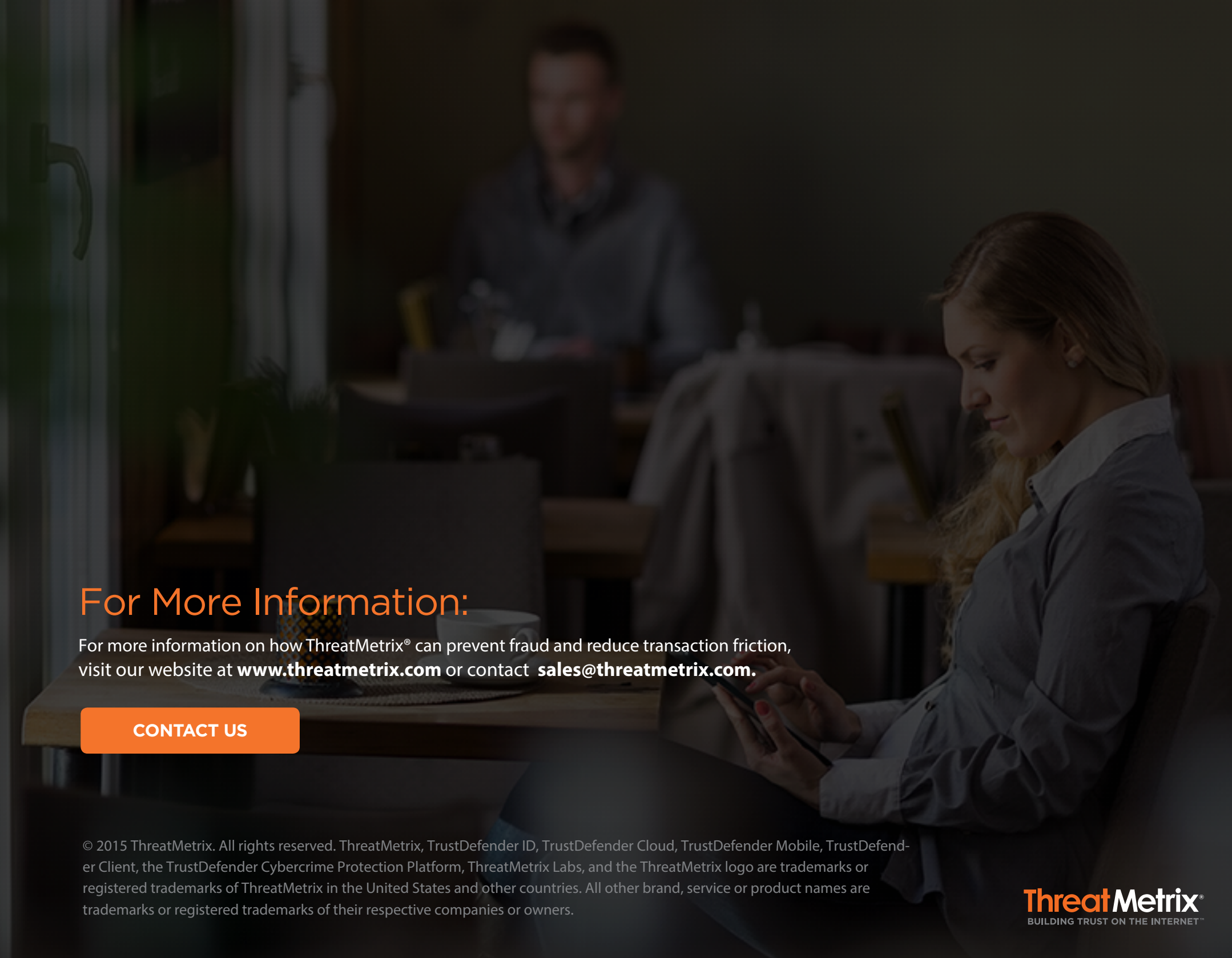
Identity Spoofing: Using a stolen identity, credit card or compromised username / password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user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

Geographic Spoofing: Hackers hide their true locations online through use of proxies, VPNs, or by spoofing browser language or time zone settings. To eliminate false positives, geo-spoofing as defined in this analysis is when the attackers to appear to be from a different country. ThreatMetrix examines a multitude of signals to determine if the computer originating a transaction or login attempt is in a different geography than where it is pretending to be, such as time zone irregularities, but one of the most effective is the use of ThreatMetrix-patented proxy piercing techniques.

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: 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.



For More Information:

For more information on how ThreatMetrix® can prevent fraud and reduce transaction friction, visit our website at **www.threatmetrix.com** or contact **sales@threatmetrix.com.**

CONTACT US

ThreatMetrix®
BUILDING TRUST ON THE INTERNET™