iovation®

2014

MOBILE FRAUD

TRENDS & IMPACT

A GLOBAL ECONOMY IS ALWAYS IN MOTION

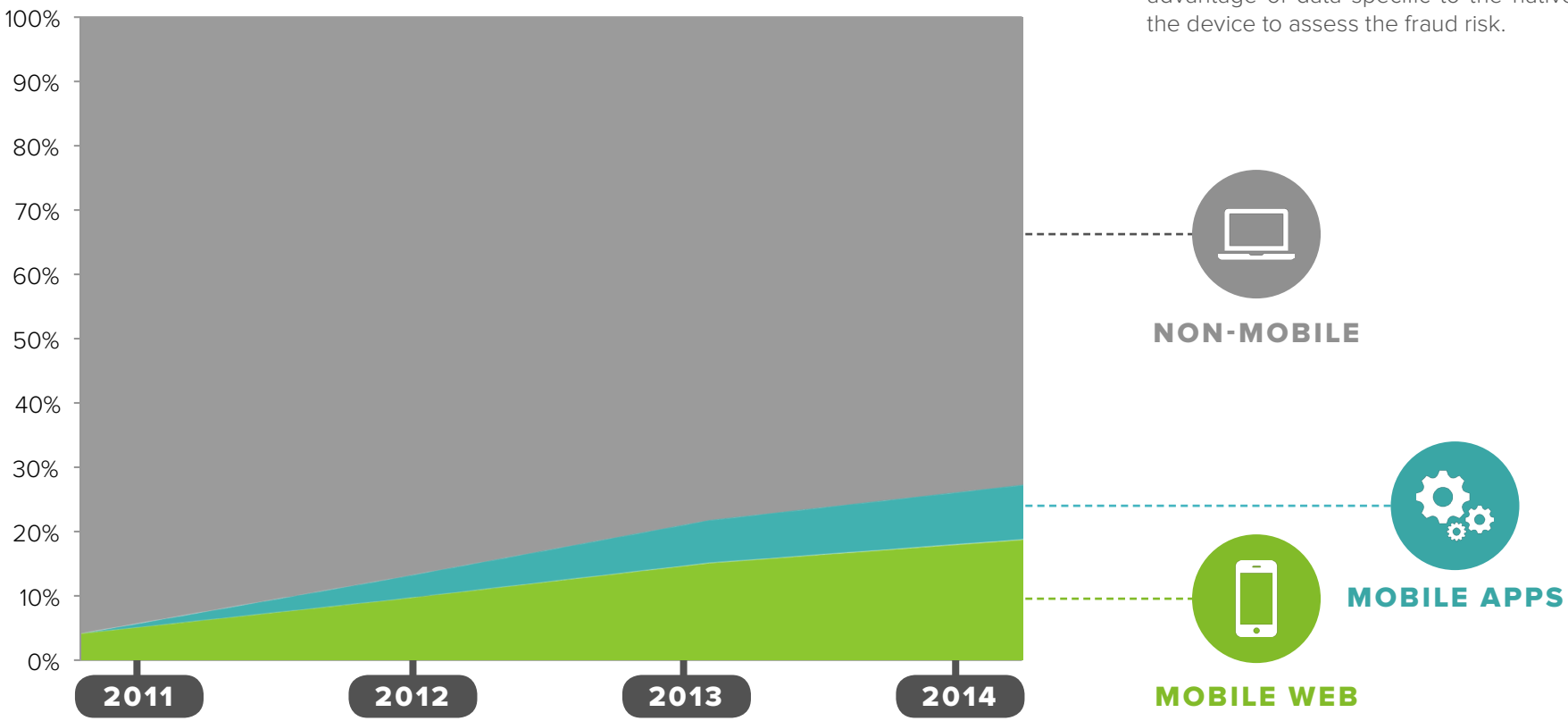
When one market closes, another on the other side of the world opens. Business today is always on-the-go, connected, it never sleeps. Mobile is how business gets done. Extending your business to the mobile marketplace requires a lot of planning and strategy. Will you deliver your service through a mobile application, browser or both? How will you secure every customer interaction regardless of the device, operating system, or network used? Fortunately, at iovation, we've got you covered.

THE RISE OF MOBILE

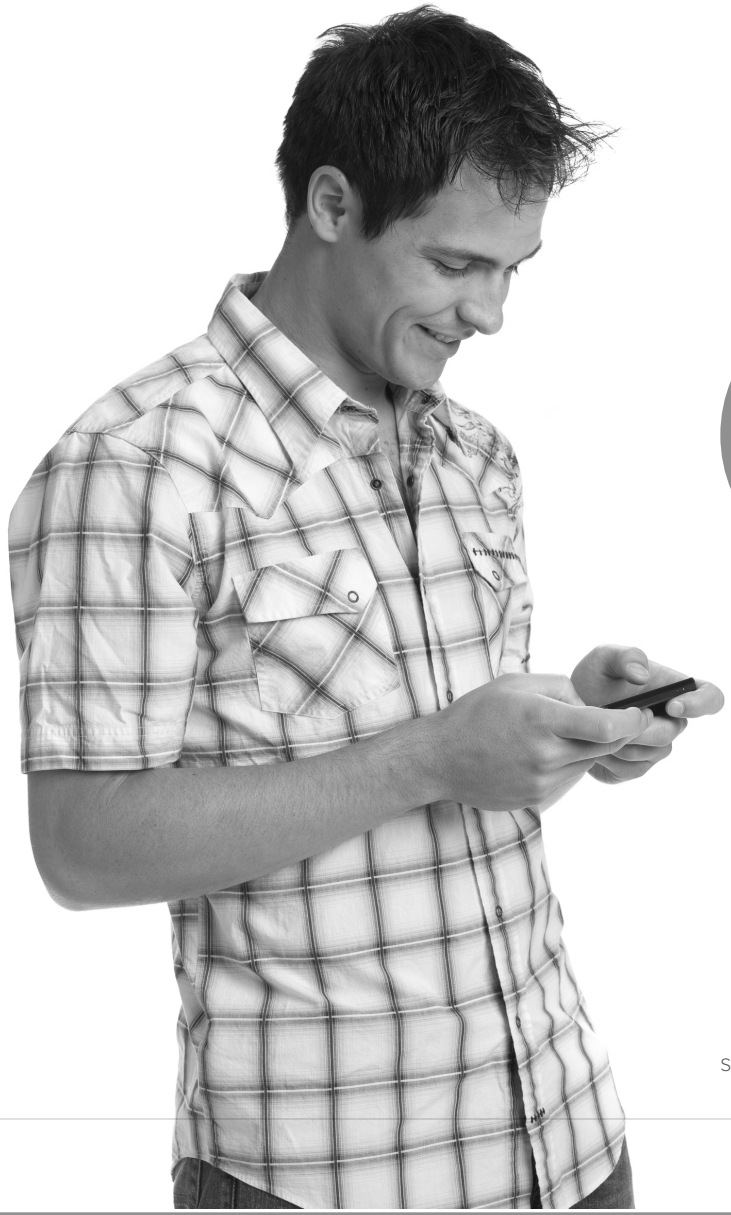
We've offered iOS and Android software development kits (SDKs) since 2011. Adoption by our clients continues to increase every year and mirrors industry adoption statistics.

We want our clients to focus on creating the best possible application they can, and leave the work of stopping fraud to us. The most effective way to do that is to integrate our SDK into your mobile application. This lets you take advantage of data specific to the native environment of the device to assess the fraud risk.

IOVATION MOBILE TRANSACTIONS TREND



WHAT IS MOBILE?



Mobile means a lot of different things to people. At the beginning of 2014 one in every five people in the world owned a smartphone and one in every 17 owned a tablet. Will the word “mobile” become irrelevant because it will be taken for granted—an unspoken understanding?

At iovation, we define mobile by operating system—such as iOS, Android or Windows Phone—independent of the device.

90%

of American adults have a cell phone

58%

of American adults have a smartphone

32%

of American adults own an e-reader

42%

of American adults own a tablet

SOURCE: PEWRESEARCH INTERNET PROJECT

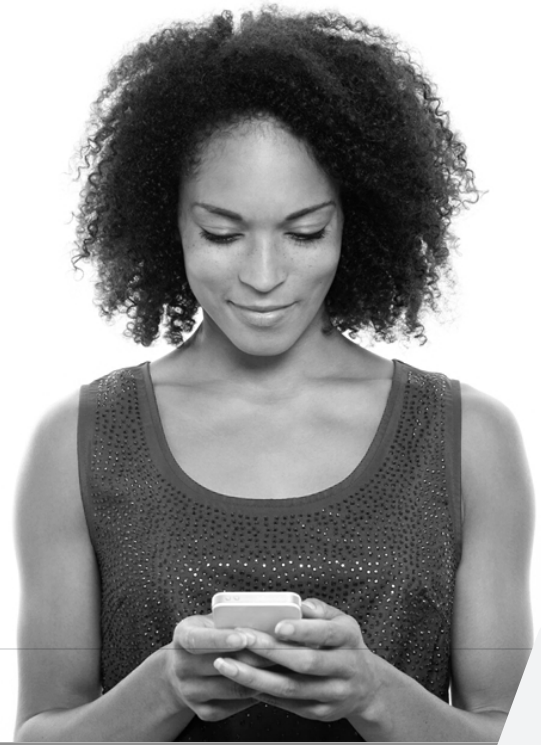
2014 MOBILE FRAUD PRIORITIES

1. Unmask disguised device attributes
2. Pinpoint mobile device and location
3. Fight account takeover across devices
4. Balance authentication with customer experience
5. Identify and protect against malware

We asked clients to tell us how mobile affects their business goals today and what their roadmap looks like in 2015. The list on the left represents their top five priorities.

Improved user experience and expanded functionality in mobile applications are the most common initiatives. They want to offer a similar experience across devices. That includes full feature sets on transactions like payments and billing, authentication, account origination and login. Understanding how, when and where customers use mobile is of key importance to their strategic efforts.

Expansion of markets through mobile requires appropriate risk mitigation for safe growth. Increased functionality can also mean increased vulnerabilities that can result in becoming a target of cybercriminals.



WORLDWIDE SMARTPHONE FORECAST BY MARKET SHARE

Analysts predict that worldwide growth will begin to slow this year as mature markets become saturated. This accounts for the slight decline in Android and iOS operating systems by 2018.

Operating System					OTHER
2014	78.9%	14.9%	3.9%	1.0%	1.3%
2018	76.0%	14.4%	7.0%	0.3%	2.3%

SOURCE: IDC WORLDWIDE MOBILE PHONE TRACKER

MARKET SHARE IS ONLY PART OF THE STORY

There's market share and then there's usage. Here's a snapshot of iovaton's global transaction data by operating system. Our clients currently see more transactions driven by Apple's iOS. That may change in the future with Android's command of market share. One thing is certain—iovation will be one of the first to see the trend.

iovation's Device Usage by Operating System

				BlackBerry	OTHER
2014	37.47%	59.6%	1.01%	0.87%	1.06%

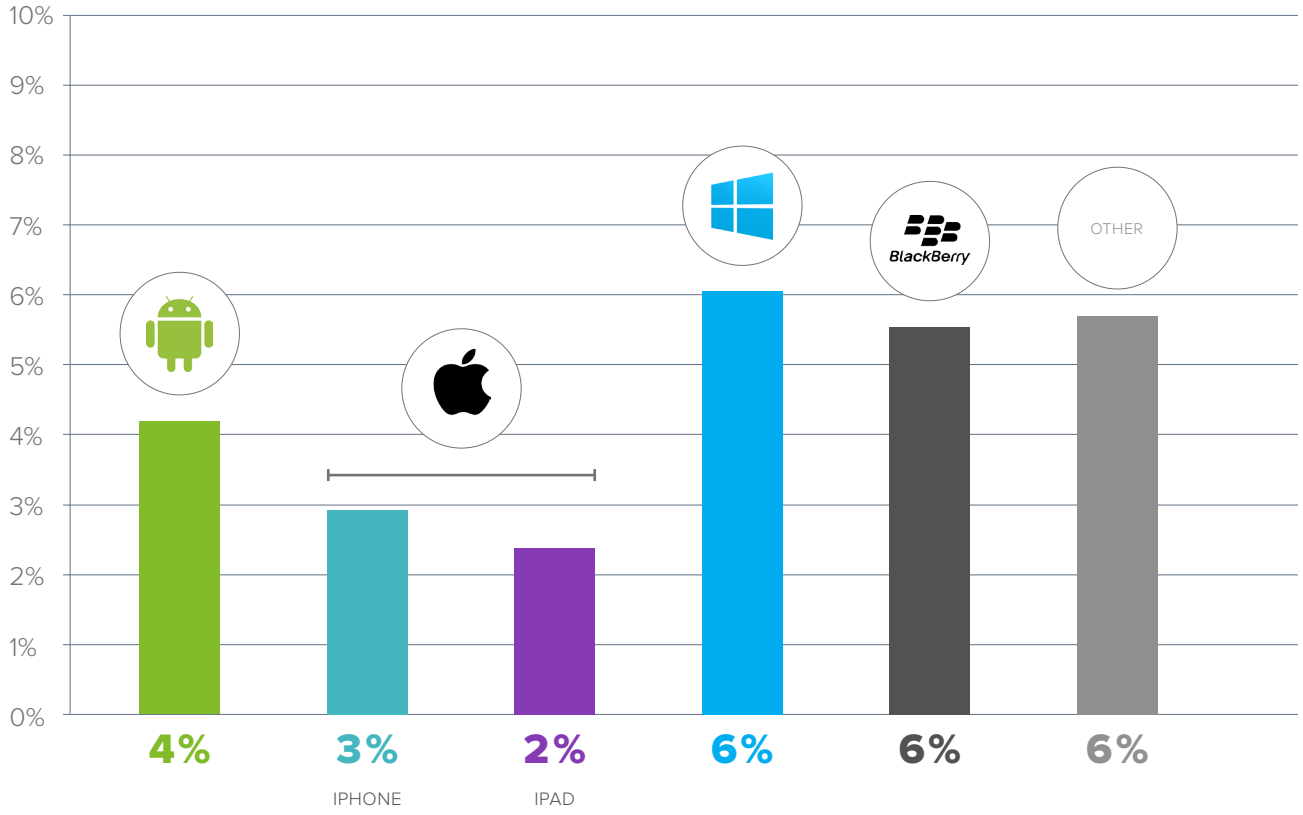
THE FRAUD RISK OF MOBILE

Identity theft, account takeover and stolen credit cards are all serious threats when you do business online. Any Internet-enabled device can be an instrument of fraud in the wrong hands. That's why real-time insight, into the history and current connections of a customer through all of their devices, is critical to assessing risk with a high degree of certainty. Device identification and reputation provide actionable, relevant data to protect your business whether a device is mobile or not.

Our customers put fraud strategy into action with business rules that can reduce review queues. No two businesses are the same. What might be considered low risk by one company may be high risk for another. The power to customize business rules creates fraud solutions targeted to the unique needs of each company. This chart defines risk as a combination of mobile transactions that have either been denied or flagged for review.

IOVATION 2014

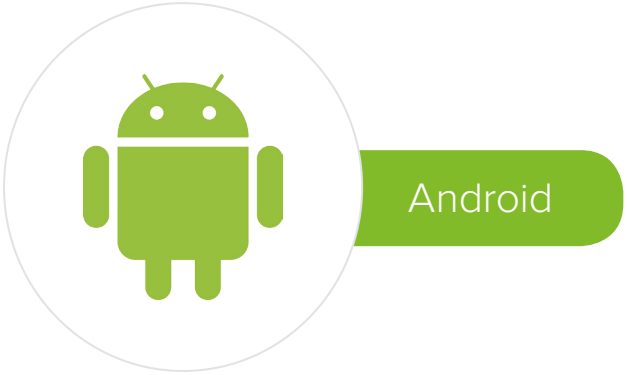
Percentage of High-Risk Mobile Transactions by Operating system



TOP 5 FRAUDS BY DEVICE TYPE

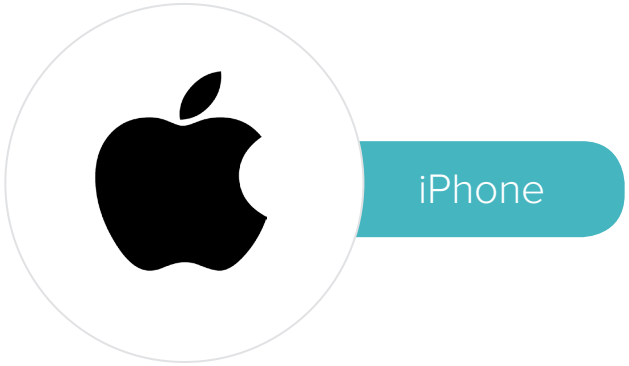
Device reputation uncovers relationships between accounts and devices across all businesses within iovation's multi-industry, global network of nearly 2 billion devices and 17 million confirmed instances of fraud and abuse.

This in-depth insight into previous fraud activity is extremely useful in weighing the risk of a transaction. It also reveals associations between devices and accounts that were previously hidden.



Android

1. CREDIT CARD FRAUD
2. INAPPROPRIATE CONTENT
3. PROMOTION ABUSE
4. SPAM
5. ACCOUNT TAKEOVER



iPhone

1. CREDIT CARD FRAUD
2. SPAM
3. TRUE IDENTITY THEFT
4. INAPPROPRIATE CONTENT
5. ACCOUNT TAKEOVER

iPad

1. CREDIT CARD FRAUD
2. SPAM
3. INAPPROPRIATE CONTENT
4. PROMOTION ABUSE
5. ACCOUNT TAKEOVER

WHERE DOES MOBILE FRAUD LIVE?

Mobile application usage has clearly taken the lead over mobile web in the United States, garnering 86 percent* of the average mobile consumer's time. The majority of that time is spent on games and social networks.

It's interesting that iovation's data shows high-risk transaction percentages are still greater on mobile web than mobile applications. When we compare Android and iOS mobile application transactions, Android is four times more likely to have high-risk transactions. This seems to support the industry consensus that iOS is a safer environment than Android, although no mobile device is completely risk-free.

MOBILE WEB 0.41%

MOBILE APPS 0.32%

MOBILE WEB 0.28%

MOBILE APPS 0.08%

*FLURRY.COM

TWO APPROACHES

HOW DO YOU DO MOBILE?

Browser-Based

Browser-based transactions travel to a web server the same as a traditional computer. That means on initial contact the device is identified and then subsequently recognized on any return visits to the site. Device reputation reports if the device accessing your website has a known history of credit card fraud, identity theft, account takeover or triggers risk factors unique to your company.

Mobile Applications and SDK

Mobile applications send data directly to a server, not through a website. Device intelligence works just as effectively with SDK and mobile application integration. SDKs take advantage of the application environment to collect additional device identification data to weigh mobile risk factors. For instance, GPS compares the location provided by the user to their actual location. A jailbroken or rooted device can indicate either a malicious or bogus version of the application and is also an added fraud risk factor.

IOVATION'S VIEW OF MOBILE TRANSACTIONS

60%

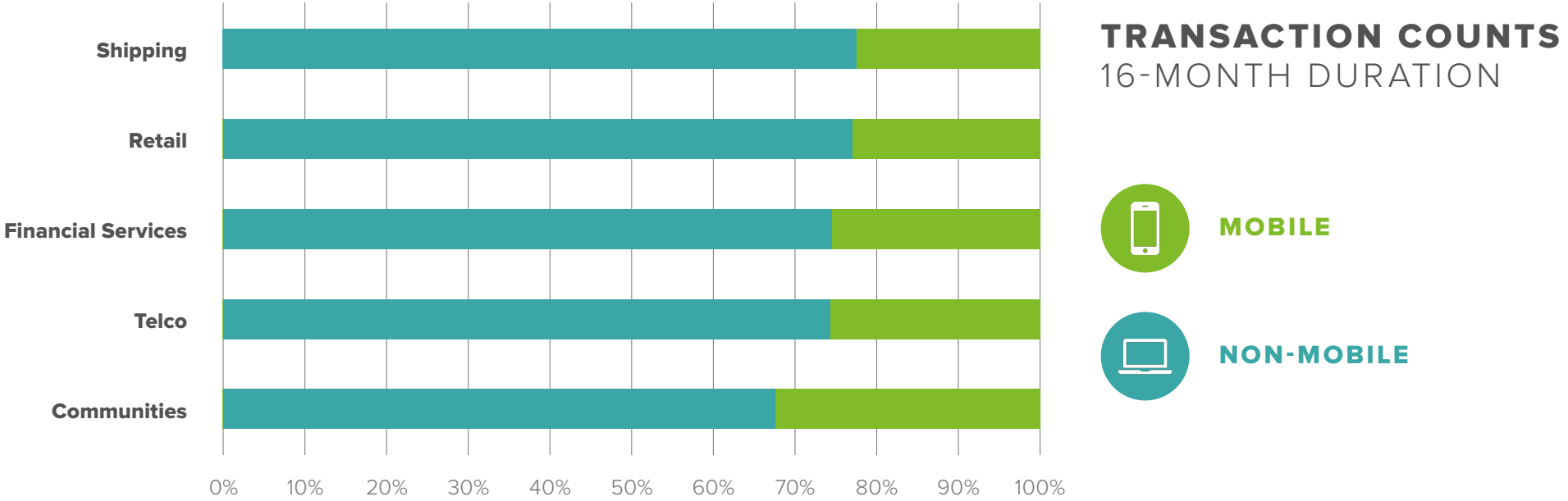
BROWSER-BASED

40%

MOBILE APPS

THE BUSINESS OF MOBILE

Mobile transactions continue to grow across most industries. Usage and adoption rates may vary by industry but all online businesses are touched by mobile devices. Online communities, such as social networks and dating, see high mobile usage rates. Banking customers use mobile to check account balances, make deposits and initiate transfers. Within the retail industry, in addition to product research and price checking, more purchases continue to be completed on mobile.



TRANSACTION COUNTS
16-MONTH DURATION

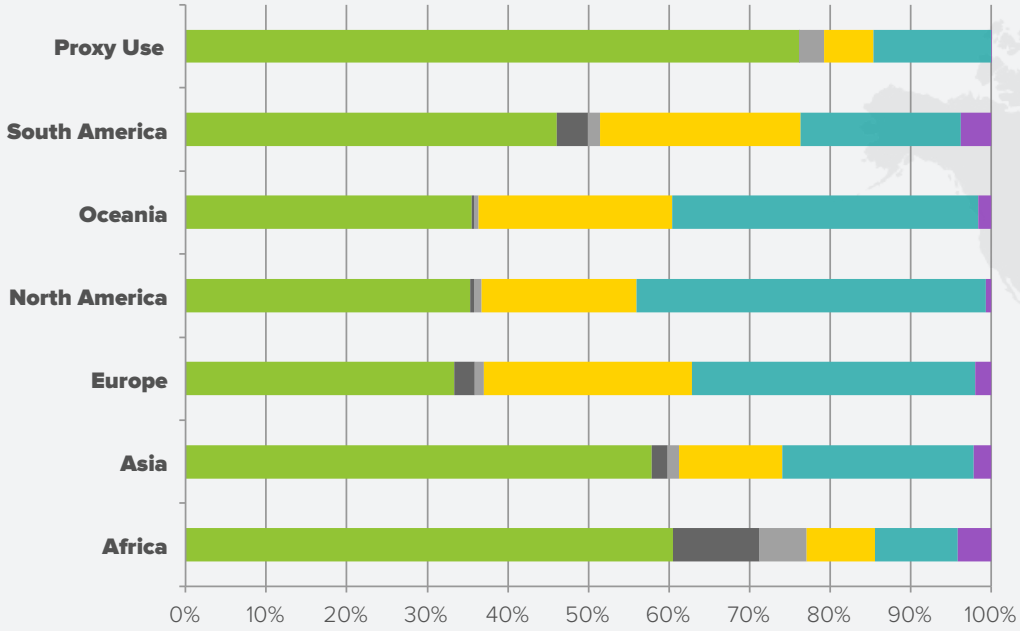
MOBILE

NON-MOBILE

THE GLOBAL REACH OF MOBILE

As mobile matures we should expect to see greater integration of smartphones for authentication purposes. It's likely that text messages, QR codes or behavior based data will be used routinely for two-step verification. Data stored on a smartphone, like songs and photos, can be used to give a business greater assurance that a customer's identity has been accurately verified. In the future, more businesses may ask customers to register their mobile devices to help stop fraud and protect their identity.

As the mobile market continues to grow, with even greater adoption of devices like tablets, insight into those devices will be crucial to fraud prevention. Device intelligence reveals the reputation of new devices based on their relationship to other known devices and accounts. This provides a layer of security that allows companies to safely conduct business online in this increasingly large and global mobile space.



MOBILE OPERATING SYSTEMS BY CONTINENT

- ANDROID
- BLACKBERRY
- OTHER
- IPAD
- IPHONE
- WINDOWS

ABOUT IOVATION

iovation protects online businesses and their end users against fraud and abuse through a combination of advanced device identification, shared device reputation and real-time risk evaluation. More than 3,000 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of Internet devices and the relationships between them to determine the level of risk associated with online transactions. The company's device reputation database is the world's largest, used to protect more than 10 million transactions and stop an average of 200,000 fraudulent activities every day. The world's foremost fraud experts share intelligence, cybercrime tips and online fraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network. **For more information, visit www.iovation.com**.

GLOBAL HEADQUARTERS

iovation Inc.
111 SW 5th Avenue, Suite 3200
Portland, OR 97204 USA

PH +1 (503) 224-6010
FX +1 (503) 224-1581
EMAIL info@iovation.com

UNITED KINGDOM

PH +44 (0) 7429 761144
EMAIL uk@iovation.com

FRANCE

PH +33 (0)6 69 79 12 33
EMAIL france@iovation.com