WHITE PAPER

Fighting Mobile Fraud

Protecting Businesses and Consumers from Cybercrime

iovation®

Table of Contents

Executive Summary

In today's increasingly interconnected and social world, mobile devices are an integral part of people's lives. From smartphones to tablets to feature phones, mobile usage is growing steadily, fueled by the popularity of social networking, mobile and Internet apps, multi-media entertainment, online banking and e-commerce.

As the growth in mobile devices creates new opportunities for consumers and businesses alike, there are also new threats emerging. This paper examines the quickly evolving mobile landscape, the business and technical decisions and tradeoffs companies will have to make to address the risk of fraud in the mobile channel, and how iovation Fraud Prevention supports these decisions.

While only 0.65 percent of all mobile transactions processed by iovation were denied at transaction time, 9.5 percent of them were sent for further review. Further, we measured a 318 percent increase in the instance of mobile fraud reported during that period based on year-over-year denial rates. We see this as a clear indicator that managing mobile fraud will continue to move to center stage as mobile use grows and the technology quickly evolves.

Introduction

Financial institutions, eCommerce retailers, social networking sites and other providers of mobile-enabled applications and web-based content are in the early stages of developing mobile fraud and risk strategies. One of the challenges is how to implement an effective defense across channels (online, mobile, physical branch/retail) while maintaining a single, comprehensive view of the consumer. Organizations want to recognize returning customers and offer them as many services as possible while balancing risk management measures.

Gaining a real-time view of the customer can be achieved by using advanced device intelligence, which links together devices and visitors even when they have not self-identified. When that perspective is combined with reputation insight that includes your fraud experiences with this customer as well as other trusted businesses, risk management accompanies the best customer experience.

In many cases, mobile is simply an extension of the Internet channel (rather than a completely separate channel of operations), with all of the inherent issues that already exist for online operations. However, mobile interactions require special marketing and operational consideration. Decisions include which services to offer via applications as opposed to a browser, and how to measure and address fraud and abuse in the mobile environment.

In making these decisions, organizations have to consider what the real threat level is versus what is perceived, the business exposure, how to protect the customer experience, what is the right level of detection and control, and the level of complexity required to integrate chosen detection solutions into their security model.

The Challenge

Growing Mobile Usage and Innovation = Increasing Fraud Risk

More and more, mobile devices and applications are becoming an integral part of people's lives. According to researchers, more than half of all American adults[1] and at least 46 percent of Europeans[2] have a smartphone. Analysis released by Nielsen Mobile Insights in May 2012 points to the expanding market share of the top three providers of smartphones[3].

- Google Android ranked as the top smartphone operating system with 48.5 percent market share.
- Apple iOS held the No. 2 position with 32 percent of the smartphone market, not inclusive of their overwhelming tablet market share.
- RIM ranked third with 11 percent share, followed by Windows Mobile at 4.1 percent.

According to a Gartner study, tablet sales are estimated to increase worldwide by 100 percent from the previous year to 118.9 million tablets by the end of 2012[4]

Market share distribution of smart mobile devices

As mobile takes off, new device types are being introduced to allow Internet access from an increasingly wide variety of locations, including your car and TV. In fact, 73 percent of new TV buyers now opt for

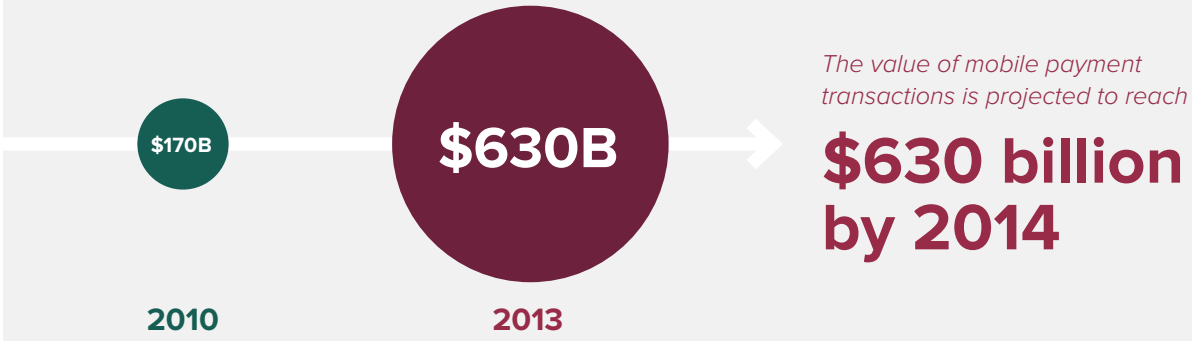
1 "Nearly half of American adults are smartphone owners," Pew Research, March 1, 2012
2 "Mobile Benchmark Data for the European Market," ComScore Mobile Lens, April 2012
3 "America's New Mobile Majority: a Look at Smartphone Owners in the U.S.," Nielsen Media Research, May 7, 2012
4 "Forecast: Media Tablets by Operating System, Worldwide, 2010-2016, 1Q12 Update," Gartner, April 10, 2012

an Internet-connected TV[5] , and it is estimated that by 2016 there will be 92 million Internet-enabled vehicles on the road[6].

While keeping in touch through social networks is one of the most popular uses for mobile devices, gathering information, buying goods and managing money is on the rise. Smartphones and tablets offer an easy-to-use interface.

The value of mobile payment transactions is projected to reach almost $630 billion by 2014, up from $170 billion in 2010[7].

Increased value of mobile payment transactions



Mobile commerce is not the only application that is growing exponentially. Mobile banking is expanding by more than 40 percent year-over-year and is expected to surpass traditional online banking by 2020[8]. This growth is driving banks to continue to invest in mobile banking solutions. While the majority of consumers use their mobile devices to simply log in and check account balances and information, the financial services sector is introducing more services like money transfers, bill pay and check deposits that take advantage of mobile platforms.

Keeping Pace with Mobile Innovation

Other innovations that bring mobile phones into the commerce world include card readers, enabling any business—from a retailer to a neighbor holding a garage sale—to accept payments from virtually anywhere from their phone. Near Field Communications (NFC) is another innovation that is migrating to mobile. With NFC, embedded chips allow for "brush-by"-type applications that can make payments, pass along data or receive information. NFC is primarily available today in chip-enabled smart cards or credit cards, but is expected to be integrated into the mobile handset and to become a standard feature of smartphone payment applications for subways, parking meters or vending machines.

5 "Smart TVs Outpace 3D TVs This Holiday Season," Parks Associates, December 19, 2011

6 "Telematics ~ The Route Ahead," Juniper Research, March 13, 2012

7 "Mobile Payments Markets: Strategies & Forecasts 2010-2014," Juniper Research, May 1, 2012

8 "2012 to 2021 Online & Mobile Banking Forecast," Online Banking Report, January 6, 2012

All of these innovations offer businesses attractive opportunities to save costs and automate processes while providing convenience for consumers. But the growth in mobile computing will also expose consumers to new risks.

iovation has witnessed a one-thousand percent increase in mobile transactions since the company started tracking mobile commerce in 2004. From January 2012 to June 2012, the company has tracked a 55 percent increase in mobile transactions. Corresponding with the mobile transaction explosion, iovation has documented an increase in mobile fraudulent activity. As more consumers conduct business and share personal information through mobile devices, fraudsters are becoming more adept at collecting personally identifiable information. Devices are being compromised through cyber-eavesdropping, identity theft and malware infections.

A recent report from Javelin Strategy & Research stated that 7 percent of smartphone users were victims of identity fraud compared to 4.9 percent of the general population[9]. The same study showed that a surprising 62 percent of smartphone users don't lock their devices with any password or code, while 32 percent admitted to saving passwords and other login data on their mobile devices.

Malware targeting Android smartphones increased...

400%

between the summer of 2010 and spring of 2011 according to Juniper Networks' "Malicious Mobile Threats Report."

In addition to weak security measures by mobile users, mobile devices typically lack the security measures that are more common on home computers, such as firewalls, network security, and anti-virus software.

Business Challenges & Decisions

While the concern over exposure to fraud is greater than its actual occurrence today, fraudsters are expected to increasingly focus on mobile devices—both as a target and as a tool.

As in any security model, a layered defense is the best defense, especially as criminals seek out points of weakness. Retailers, financial institutions, social networking sites and other providers of mobile-enabled applications and content can help protect consumers—and themselves—with a mobile fraud detection strategy that integrates with security measures within the Internet channel, and across other channels. Being able to correlate transactions based on the devices used, and tie together the device inventory of an individual (computer, tablet, mobile phone, etc.) strengthens the defense by providing a comprehensive view of the customer.

Still, challenges to securing the mobile channel exist both from a business and technical perspective, and companies will need to weigh all factors to determine the right security strategy—including

9 "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier," Javelin Strategy & Research, February 2012

customer experience, technology platforms, integration and the right level of detection and control. Following are some of the key factors to consider.

App vs. Browser

Mobile apps can be built with more security, and mobile browsers are 'thin' compared to computer-based browsers. But while apps can gather more information about the phone, penetration is lower and different versions are needed for each platform—phone, tablet or operating system. Browser-based experiences are more universal, do not require a download and do a better job keeping up with new models and operating system versions. While a year ago it seemed that apps were winning the 'popularity' race, we are now seeing more preference towards a browser-based experience, which results in more need for options for securing browser sessions.

Tablets vs. Smartphones

While both tablets and smartphones are driving the explosive growth in mobile computing, each device has different user experiences and consumption patterns. We do not know whether tablets will be the preferred platform for, say, banking while smartphones are used for shopping, but clearly the form factor will impact the feature set. With so many mobile devices being used for so many different functions, it's important to be able to track behavior on multiple devices, no matter what they are.

"Stay at Home" Mobile Usage

Not all mobile devices are used on the go. In fact, many mobile users browse, get or share information, shop, or check accounts from the comfort of their couch. This behavior often occurs through a "static" WiFi connection rather than through wireless carriers. While security measures implemented through wireless carriers is important, a business can't be totally reliant on carriers for all mobile device security.

Cross-Channel Consumer Touchpoints

How does a business create a unified view of the consumer when engagement can come in a variety of methods and channels—checking account balance via smartphone, calling customer service by landline, and making payments on the home or work computer? With an ever-expanding range of consumer interaction points, it's important that your tools can help you facilitate communication across the organization—for both marketing and fraud prevention. (See the section 'The iovation Solution' on page 10 for how iovation provides this unified perspective.)

Account Takeover (ATO)

Fraudsters know that it is generally easier to take over an account by phishing, spear phishing (targeting an individual) or smishing (phishing via a mobile device), than to open a new account using a real or 'synthetic' identity, which is why the risk of account takeover is one of the most alarming trends in fraud. Recent hacking events, including the LinkedIn password list breach in June 2012, illustrate the first step of an ATO attack. With information such as birth dates and home addresses relatively available through a consumer's social media activity, data stolen from unsecure sources or tricking a consumer into sharing them (phishing), cyber criminals have an easy path to account takeover.

Furthermore, account takeover at your business is not the only issue that can be negatively impacted. One of the key methodologies for transaction verification has been the use of mobile phone and text features for customer validation—SMS messaging or automated voice calls are now effectively in use in second factor authentication processes. Fraudsters understand that as well, and have been using simple phone porting (asking the carrier to forward or reassign the number to another device) to intervene in that process.

Measuring variances in common behavior is being used to trap account takeover as well. Examples of behavior that might trigger an additional review include a funds transfer at 3:00 am when all other transfers have occurred during the day, or account access from a foreign country.

Avoiding Undue Customer Friction

While businesses need to protect themselves and their customers, consumers may flee if the security friction gets too high. While consumers have indicated that they expect the enterprise to protect them, studies show that too many levels of authentication, including multiple security questions and codes, result in lost customers when the digital experience becomes too arduous. Finding the optimal balance between security and customer experience is key.

FFIEC Compliance

In the United States and a few other jurisdictions, mobile fraud strategies for banks, credit unions and other financial institutions will need to meet revised FFIEC guidelines issued in 2011 . These guidelines, as outlined in the "Supplement to Authentication in an Internet Banking Environment," are designed to protect financial transactions from sophisticated cyber criminals. They require financial institutions to:

- Assess online banking risks on a regular basis.
- Implement layered security measures, including complex device identification and device reputation risk assessment to help detect fraud.
- Promote fraud awareness among consumers and members through educational campaigns.

Malware Detection

Malicious software, often referred to as malware, is an increasingly common method used by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Cyber criminals are getting consumers to download malware on their mobile devices through such activities as downloading of mobile apps, surfing on public (and insecure) WiFi access points, text messaging, and more. Without firewalls and other security measures that are more standard on home computers, mobile devices are at high risk for downloading malware.

Mobile Device Theft

The popularity of mobile computing and the devices that enable it have also increased the value associated with smartphones and tablets. Theft or loss of a mobile device can compromise a consumer's information, particularly when passcode locks are not routinely used, or when there is stored account information anywhere on the device. Common best practices in mobile security include

never allowing the transmission of passwords or user names between consumers and businesses via text messaging, and not storing passwords or identifying information about consumers or accounts anywhere on phones. The financial services industry is leading the way in protecting consumers' accounts when their mobile devices are reported stolen, and handset manufacturers are at work on developing a "stolen phone" database as another defense mechanism in the war on fraud.

The iovation Solution:

Protecting Businesses From Online Threats In Real-Time

iovation Fraud Prevention is a cloud-based service that actively manages nearly a billion unique devices across a broad range of industries around the globe, and has protected more than 8 billion online transactions for its clients. Identifying the device used to commit fraud is an effective way to root out fraud—and one that iovation has offered its clients since 2004. iovation has seen significant growth in mobile transactions, especially over the last few years.

- As referenced earlier in this whitepaper, in the first six months of 2012, iovation reported a 55 percent increase in mobile transactions.
- From May 2011 to 2012, iovation saw triple digit transaction volume increases on the most popular mobile devices.

PLATFORM	MAY 2011	MAY 2012	% CHANGE
iPhone	2,861,506	7,187,372	151%
Android	2,160,060	5,617,141	160%
iPad	1,042,402	3,760,893	261%

Web visitors are using mobile devices to interact with online communities such as social networks and dating sites, and are doing more and more business with online retailers, gaming sites, and financial institutions. While iovation records and shares over 40 different types of fraud and abuse events, approximately 20 of those have been involve mobile usage. Ninety percent of all fraud attempts reported from mobile devices have included credit card fraud and account takeover attempts.

One advantage businesses gain through iovation is to use device-based data to "stitch" together the network of related devices that represent either a user or a group of users—if transactions are conducted by a phone that is in close proximity to a home PC, chances are the user is at home and risk of fraudulent activity is lower. This ability to associate devices together over time, to build a device-based 'network view' of the customer is one of the most powerful features of ReputationManager 360.

Fraud Protection for Mobile Apps and Browser

Traffic originating through a browser as well as those coming through an application is protected by iovation. Our Fraud Prevention solution identifies devices accessing your site via mobile browser, and its native software development kits (SDKs) are available for inclusion with mobile apps. Its mobile iOS SDK code meets Apple's rigorous standards for iPhone and iPad applications, to help make the approval process quick and easy. The user experience is unaffected by either approach as iovation makes every effort to not impact the customer experience.

The company was the first vendor to introduce iOS and Android SDKs at the beginning of 2011 and is the only vendor with SDKs deployed by customers that enable strong device identification for applications. It develops SDKs for mobile platforms that have a significant market share, an active app market, and show signs of healthy growth. iovation plans to support Windows Mobile when penetration ramps up, which is expected to occur early 2013.

Addressing Business Challenges Across Industries

Hundreds of online retailers, banks, social media sites and other businesses utilize iovation to keep up with the always-evolving methods cyber criminals are using to conduct online fraud.

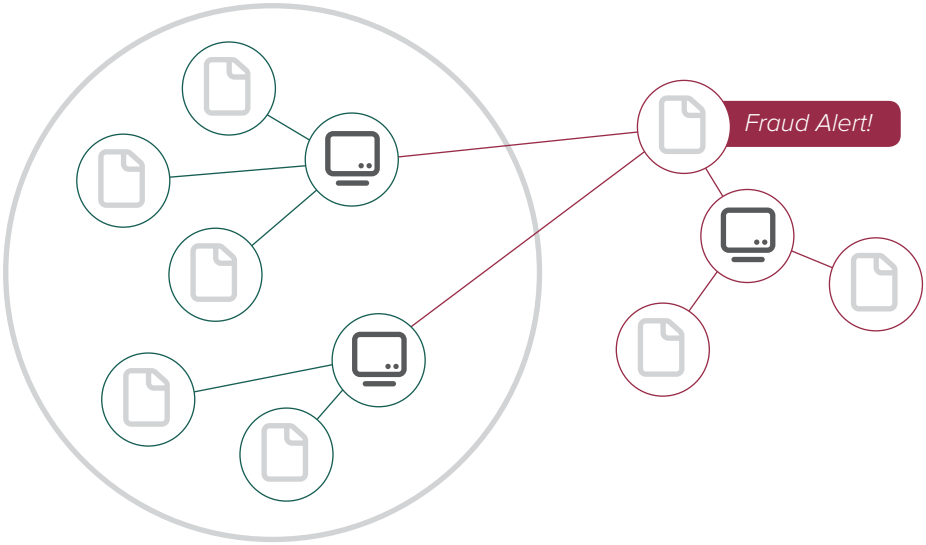
BUSINESS CHALLENGE	IOVATION SOLUTION
Need fraud detection for both mobile apps and mobile browser	Supports both browser and app-based access and was the first to release SDKs for iOS and Android apps.
Managing access to an account via multiple device types such as tablets, PCs, smartphones	Supports all major mobile operating systems and devices, and is continually adding new devices to our recognition algorithms.
Uncovering the true location of mobile devices as they are not always 'on the go'	Offers geolocation capability to correlate transactions to devices used, and tie together the device inventory of an individual (PC, tablet, mobile, and others).
Understanding customer associations across channels, including web/mobile, brick-and-mortar, and call centers	Covers mobile and wired web and links the devices used in both channels. The customer experience from brick-and-mortar and call center can be extended into the web/mobile channel.
Detecting and preventing account takeover or hijacking attempts	Shares customer-reported events of account takeover activity to block future fraudulent transactions and offers out-of-band (OOB) authentication to further protect consumers.
Minimizing friction for good customers	Customer experience must be considered, iovation operates behind the scenes and allows the bank or merchant to control the flow when risk is present.

Meeting FFIEC compliance guidelines	Takes complex device identification much further by layering device histories, geolocation, velocity checks, risk profiles, device anomalies, OOB authentication—offering a complete device reputation.
Detecting malware on compromised mobile devices	Addresses malware injection and transaction hijacking with OOB authentication, allowing banks to identify and stop transactions not intentionally initiated by the customer.
Understanding when mobile devices are stolen	Stolen phone database being developed by carriers are under consideration as a data source for iovation's real-time business rules.

iovation Fraud Prevention: How Does It Work?

While there are many options for device identification, iovation is the only provider of true device reputation. iocation Fraud Prevention exposes iovation's unique view of Internet activity to deliver actionable intelligence about the trustworthiness of the individuals at the other end of an Internet transaction. In doing so, the service analyzes device attributes and anomalies, consumer history across a broad swath of industries, and the network of associations that have been built over time. Each transaction is processed, scored and returned with device and risk data including an allow, review or deny recommendation.

A key differentiator of the iovation solution is its ability to include mobile devices in its vast network of associations. In this complex "association network," iovation associates groups of devices that are related to one another by looking at common account access for its customers; for example, if a user logs into his bank account from a home computer, work computer, and a smartphone, the iovation solution can show its client, the bank, that these devices are associated. Knowing these network of associations helps to effectively identify fraudsters working in collusion and efficiently shut down fraud rings at once.



The diagram below shows a network of 3 associated devices connected through access to 8 accounts. One account was flagged for fraud, raising the risk level of the network.

Today, iovation recognizes mobile transactions by operating system and platform, including iPhone, Android, iPad, Blackberry, MIDP, Windows Mobile, iPod, HP Mobile, and others. The most commonly used devices on its clients' sites are the iPhone, iPad and Android operating system-based devices.

A View to the Future: Technical Features and Capabilities being added to Fraud Prevention

FEATURE	IMPACT
Phone identification—phone type such as landline, mobile, VOIP, prepay	Different types of phone are associated with different levels of risk. Most risky are VOIP and pre-pay as they are most difficult to tie to an individual and are easiest to acquire and change.
Authentication—using a pre-stored phone number (provided during registration) to validate a transaction	Second factor authentication is an effective OOB process, allowing the merchant or bank to validate that a) the correct user is interacting with the business, and b) they intended to complete the transaction, thereby defeating MITM/MITB attacks.
Verification—using a number provided at the time of the transaction to send a one-time password (OTP) via SMS or automated voice call	Validates the transaction and allows the addition of phone information for additional screening.
Knowledge-based authentication (KBA)	Ensures that consumers are "who they say they are." This process is significantly more effective when used in conjunction with device reputation.
Track usage patterns and fraud trends by platform and device type	Allows iovation to extend powerful anomaly detection even more deeply into mobile devices.

Protecting Your Business Today

Where to Start

Developing a mobile fraud strategy can feel like a daunting task, especially given the number of business and technical factors to consider and the quickly evolving mobile technology landscape. However, there are a few areas where you can get ahead of the curve with already deployed and proven fraud detection solutions.

A mobile fraud prevention strategy that builds on and leverages the strategies in place for the web is a best-case scenario. iovation Fraud Prevention is the only service that actively builds and maintains associations between all devices accessing an account—linking computers, tablets, mobile phones so your risk strategies cross the channels available to your customers.

When it comes time to confirming a customer's legitimacy, phone authentication helps verify the identities and devices of users accessing an online service. This can be especially useful considering that identity theft and account takeover are the two most common types of fraud facing mobile carriers. Authentication can also assist in stopping so-called "friendly fraud," where criminals prey on family or friends to steal or take over their identities to perpetrate fraudulent activities, such as setting up new accounts or conducting transactions. Friendly fraud is a growing issue for businesses, as most merchants "own" all of the risk and loss.

While authentication is one component of an effective fraud management approach—which should also include device identification and re-recognition, pattern matching, risk scoring, and reputation sharing—it can be a critical first step to implementing a defense-in-depth strategy for fraud and abuse mitigation.

Conclusion

The mobile channel will continue to grow, as will the opportunity for fraud. Fraudsters are always looking for ways to exploit points of weakness and are expected to increasingly target mobile devices.

The best way to fight mobile fraud is to develop a layered defense that will help you expose hidden relationships between users and devices and assess their reputations to help you know which transactions to trust. Companies need a comprehensive view of their users' accounts and the devices or channels used to access them. Incorporating device reputation into to your fraud strategy is an effective way to help prioritize and manage the mobile channel and protect against ongoing cyber attacks.

Please contact us to learn more about mobile fraud protection by emailing info@iovation.com or calling (503) 224-6010.

ABOUT IOVATION

iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, device-based authentication and real-time risk evaluation. More than 3,500 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of billions 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 15 million transactions and stop an average of 250,000 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) 800 058 8731
EMAIL uk@iovation.com