IdentityMind GLOBAL

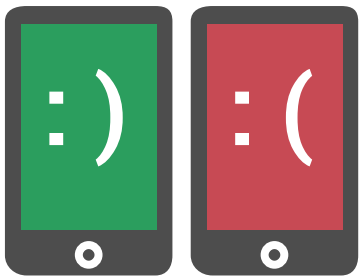
Balancing Risk Management & The Mobile User Experience

GUIDE

Digital commerce is growing rapidly worldwide, and, as it grows, so does fraud. And, for many companies, most of the fraud comes from fraudsters using a mobile device.

This guide looks at the challenges of balancing risk analysis and user experience for mobile channels. It will provide ideas on how to address the challenges of combating fraud while also maintaining a user experience that will not turn away your prospects and customers.

Part I: Benefits and Challenges of Mobile Commerce



The explosive growth of mobile commerce worldwide is both bringing in customers from previously neglected demographics (i.e. underbanked and unbanked), and catering to the large percentage of consumers who now use mobile phones to access financial services, make payments, and complete purchases.

However, this transition is bringing a new set of challenges for mitigating online fraud, and online merchants and providers of financial services need to quickly prepare for these challenges in a cost effective manner.

User Experience and Going Mobile

As with any consumer application, user experience is key, and the companies designing end-to-end user experiences for the mobile channel are the ones driving higher adoption. Most businesses have high expectations of success and are pushing to “go mobile” as fast as possible. However:

1. **Most** think their current website is ready for mobile users, which often yields a very small return. Mobile should be recognized as a new channel, separate from online.
2. **Some** take the time to adapt their website for a better user experience, creating a mobile-friendly version of their website.
3. **Few** develop a whole new user experience and new, mobile-ready website.
4. **Far fewer** develop a smart app to control the entire user experience.
5. **Very few** companies develop a user experience where payments are so well hidden that users don’t think about it.

In short, the more thought and resources you put into the end-to-end user experience, the higher your likelihood of success.

Enabling Mobile Commerce

It's important to establish a framework to analyze how mobile contributes to your current traffic and configuration. Our solution provides this, but we're not alone. Your framework should operate as a tool for analysis - to measure activity, identify areas of risk, and frame the value of different channels. Each channel should require a different approach based on the types of risk it's exposed to.
Methods of Mobile Commerce

1. Enable commerce from mobile devices (i.e. smart phones/tablets)

This describes the ability of digital commerce websites to accept consumers through mobile devices that have internet browsers. Merchants and service providers often improve functionality by reducing steps during the checkout processes, and creating mobile-friendly websites.

2. Mobile Apps

This specifically refers to providers who offer a smartphone application for mobile operating systems like iOS and Android. These applications have usually tackled user experience at a deep level, and can provide aggregated services through digital wallets.

3. Alternative Mobile Payments

Alternative methods include payments through SMS/Voice that leverage carrier billing. These include payments through SMS, but also cellular minutes as a form of currency (e.g. airtime top-up providers).

Most literature describing the risk challenges of mobile tends to focus on the difficulty of accepting payments from a mobile device. This focuses on solutions separated from the user experience and its environmental circumstances, which are important aspects to consider.

Risk Analysis Challenges

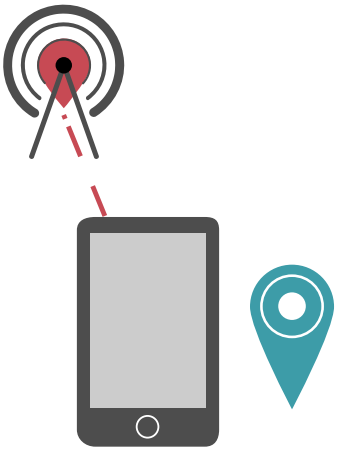
Risk analysis challenges can vary by the business, but with mobile, we've identified 5 distinct issues:

1. Expedited Checkout Experience

Typically, the higher the friction in a transaction, the higher the rate of abandonment. Since customers expect a faster user experience, and are less inclined to type on tiny devices and keyboards, mobile providers usually seek to reduce friction by limiting the amount of information required for mobile purchases. This expedited checkout experience provides less information for risk analysis.

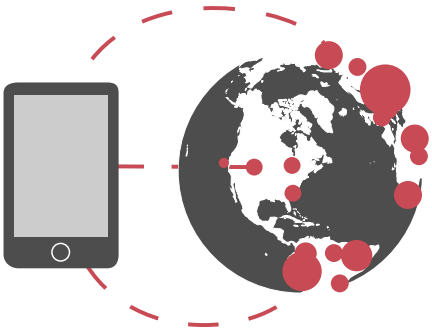
The exception to this are providers who focus on the overall user experience- collecting relevant information as a native aspect of the app.

2. Common and well-known risk analysis tools may not be as reliable



IP Geo location analysis and IP-based risk are common and very affordable tools to reduce fraud in e-commerce. However, IP addresses - the basis for IP Geo location and IP Risk - aren't reliable for identifying location on mobile devices. Carriers assign IP addresses based on "Gateways" that may be located far from where the cellular access happens. Additionally, device fingerprint technologies in mobile are less accurate than on personal computers, with higher rates of both false positives (collisions), and false negatives.

3. International Orders



International orders have higher fraud rates than domestic orders (where domestic is based on the location of the provider. We'll consider the United States as domestic). More international users now have access to the internet through smartphones than they do over personal computers (PCs), and the percentage of international orders through smart phones is steadily increasing. This makes international orders on mobile even more risky than orders from domestic mobile or international PCs.The average rate of fraud for international orders is double that of domestic orders (this is often exacerbated by fraud providers' lack of local payment and identity verification data).

4. Cross-Channel Solutions

Providers who are serious about exploring the mobile channel also tend to explore alternative payments. However, fraud tools typically do not cross over all payment channels; most fraud providers focus only on specific payment instruments (e.g. credit cards), which makes it difficult for digital commerce providers to accurately track and analyze risk.

5. Simple Measure of Fraud

Most organizations don't separate their analysis between mobile vs. non-mobile, and the overall cost of mobile fraud is therefore diluted within the category of online, PC fraud. However, public data reveals that fraud rates in mobile are double that of the web channel; it's simply more difficult to isolate and apply specific measures in this environment.

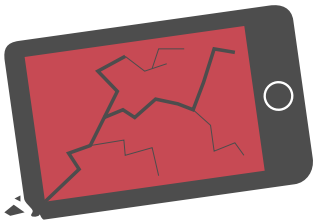
Part I Take Aways

Most companies don't realize the effort that should go into, or the benefits of designing an end-to-end user experience for mobile. Mobile should be considered a new channel, rather than an extension of online commerce. Your customers are interacting with and experiencing your site in a much different context; the more thought that goes into designing this experience, the higher your chances of success.

A proper framework should track mobile commerce separately from the start. This will allow you to segment and analyze activity, accurately measure success, and analyze risk by channel.

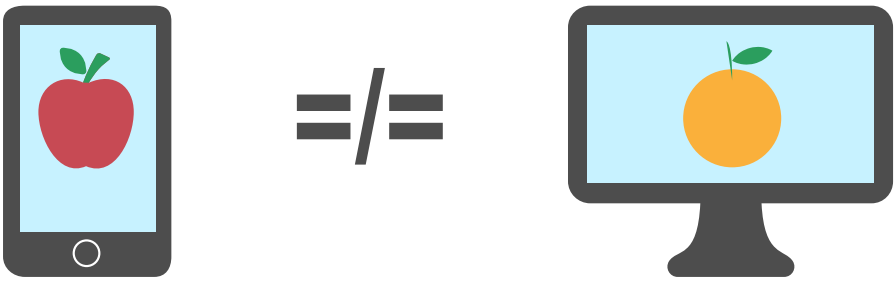
Risk in mobile is underrepresented. Traditional risk solutions are not as effective in mobile settings, providers typically require less information, and most metrics do not separate mobile fraud in their categorization of online fraud - despite the fact that fraud rates on mobile are twice that of web. By accurately reducing mobile fraud, you may significantly reduce the overall fraud rates for your business.

Part II: Common Mistakes

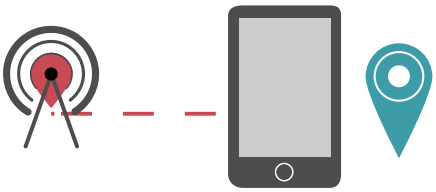


Treating mobile as a simple extension of online commerce tends to increase the risk of it. Unfortunately, that's the most common approach taken by providers. We have found four common mistakes businesses often make as they enter mobile commerce.

1. Taking the same approach as in e-commerce



Addressing mobile risk isn't the same as addressing risk in a web channel. There are always specific techniques that are more cost effective for one channel than another, and mobile is no different. Let's consider a couple of specific examples:



IP Geo location and IP-based risk are both common risk analysis tools in traditional ecommerce. However, these methods are less reliable when analyzing mobile traffic. Cell phone carriers, for example, may route mobile traffic through aggregators and gateways, which can be located far from the actual location of the mobile device.

Many businesses collect less information during the payment checkout process - for example, they stop collecting full billing address, or stop comparing billing and shipping addresses.

Many mobile apps also have access to natural information users submit to improve the app experience. This can include for example, access to phone GPS to provide maps to local stores, multiple forms of user verification at login, or maintaining a history of use that is more frequent and predictable than sporadic visits to a website. However, fraud analysts often fail to use this new information, or the tools they use can't properly apply this information to develop new fraud prevention rules.

2. Lack of Correlation

Fraudsters will use and exploit every channel they can. They will find the most vulnerable avenue and exploit it until they've exhausted the method, and the channel.

This means that for mobile - or any other channel - information should be correlated across applications and payment methods. Fraudsters who have already been recognized by your organization and exhausted one channel will likely target it from a different direction, or another payment method - in this case, mobile.

3. Common Tracking

Better decisions are always made when there's access to relevant data. Some providers may not have realized there are higher rates of fraud from the mobile channel than traditional web. Risk analysts and business owners may be looking at the overall fraud rate, but should track each channel separately to act properly.

An effective risk management program should track common patterns across as many factors as possible - by channel, product, location, payment type, time, and more - in order to analyze what combinations of factors contribute to the highest incidents of fraud. The better you know the risk signals and contributing factors, the better you can screen, and the more cost effective your program. Understanding and segmenting your traffic by mobile vs. online channel should be a factor in that tracking.

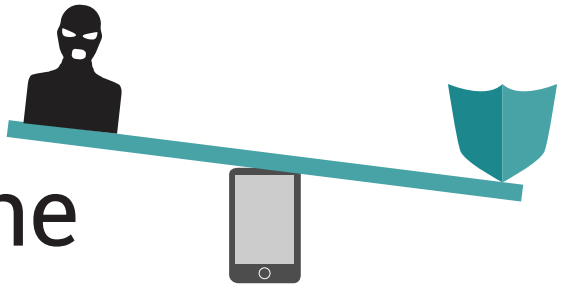
4. Acceptance of Risk

"Mobile is higher risk." Well, perhaps. But there are now cost effective tools to deal with that higher rate of fraud. There's no reason to risk revenue by simply accepting losses due to fraud, or to ignore the entire channel when there are cost effective alternatives that can help you manage that risk.

Part II Take Aways

Businesses often fall victim to these common mistakes as they enter mobile commerce. Mobile is usually treated as an extension of online commerce, which increases the risk associated with it for most providers. By treating Mobile as it's own channel, you can mitigate risk accordingly.

Part III: Leveraging the Phone



There are unique opportunities mobile presents for managing risk, and how you can use natural information from the user experience to supplement your risk program.

1. Leveraging the Phone

Apps can provide accurate location using latitude & longitude.

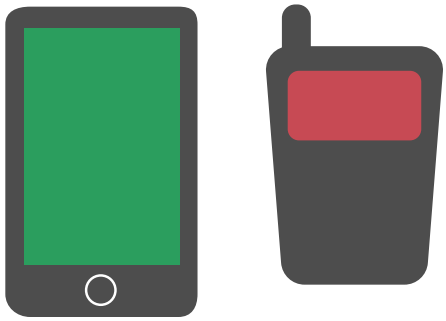
Rather than analyzing IP location for payment, many apps already collect location data to better inform the consumer of nearby stores, coupons or deals in their area, reviews, and more. In these scenarios, a device's proximity to the billing address can be a strong positive indicator. On the flip side, however, purchases outside a reasonable ratio of the billing address, or opting out of providing these details aren't strong indicators of fraud in themselves.

SMS verification

Correlating the correct phone number with an account via SMS verification helps build a strong customer relationship. While it's desirable to associate a phone number with an account, just the fact that a customer responds to SMS verification is a positive indicator, especially when responding correctly to a challenge. On the other hand, failure to verify through SMS is also a very strong negative indicator. In contrast to what many merchants believe, SMS verification usually increases customer satisfaction, especially on high value orders.

Phone type as a risk indicator

In general, prepaid phones, toll free phone numbers, and Voice over IP (VOIP) are higher risk than "normal" contract carrier phones. Voice over IP can be tricky though, as some industries- for example, online gaming- have demographics more prone to using VOIP. Phone type in these scenarios should be used in conjunction with other indicators.



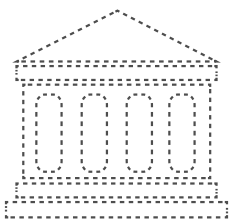
2. Leveraging the Knowledge of the User

Recycle natural user information where available

Customers tend to share more data through smart applications, where information is collected passively, and when there is an incentive to do so- such as sharing extra information to receive coupons or rewards. Much of this information can be reused for risk analysis purposes.

Carrier Data

Some providers have a level of insight into carrier data - this data can used to match subscriber and phone number.



Underbanked/Unbanked

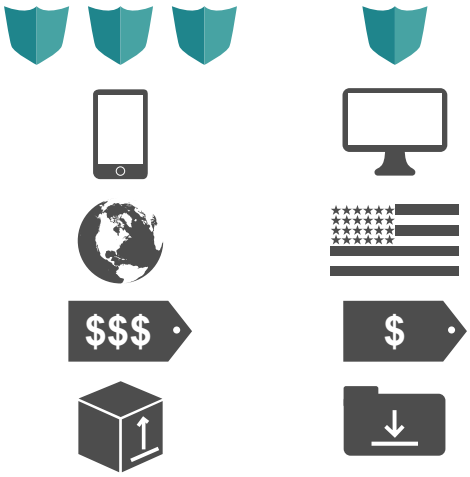
The mobile channel taps into underbanked and unbanked demographics both domestically, and abroad. Depending on your type of business, finding data partners that have visibility into these demographics can be essential.

International Identity Verification

Some countries maintain local user databases with name and address information that can be used for customer verification - find a partner with access to these databases.

3. Knowing the Risk

Discriminate by Risk



Not all transactions are created equal. It's important to segment your traffic and create profiles based on the risk they pose to your business. Analyze, and add friction where necessary. The most basic discriminations and examples include:

- Mobile vs. Web
- International vs. Domestic
- High ticket items vs. Average ticket items
- Physical vs. Virtual Goods

Payment Types

All payment types have different risk profiles - make sure you understand how to measure and translate this risk. Fraudsters will take advantage of the nuances of different payment methods and models. This also includes rewards and coupon systems, stored values, and similar programs.

Visibility across the ecosystem on underbanked/ unbanked demographics

With higher rates of unbanked and underbanked audiences now using mobile to access the financial system, it's important to find a way to verify audiences who may not be recognized in established databases. A solution like IdentityMind is an important asset in this regard.

Part III Take Aways

Mobile devices will continue to be adopted at an accelerated pace, and are already bringing new demographics into digital commerce and financial services. 52% of smartphone users with a bank account have used mobile banking, and 22% of all mobile phone owners reported having made a mobile payment according to the Federal Reserve's 2015 report. Mobile will continue to grow as a fundamental aspect of international commerce, and the most successful providers will offer high-value user experiences through sophisticated apps.

However, without an accurate understanding of risk challenges and investment into proper risk management strategies, the cost of fraud in mobile commerce will continue to hinder the ability of merchants and providers to operate cost effectively in this channel.

Conclusion: IdentityMind Fraud Prevention for Mobile

To compensate for these challenges, we've created a solution specifically for mobile providers. Our mobile fraud prevention combines superior identity verification services and technology, with fraud policies designed to accommodate mobile channels, seamless use of natural user information, and our core Electronic DNA™ to provide worldwide fraud prevention services in even the most difficult environments.
On March 31st, we announced our strategic partnership with Mozido to expand safe, secure mobile commerce around the world.

This partnership bolstered our vision, and importantly, increases our footprint in addressing the challenges associated with preventing risk on mobile platforms for payments, money transfers, and overall digital commerce worldwide.

For more information on IdentityMind and our fraud prevention services for Mobile commerce, feel free to reach out to us at **evangelist@identitymind.com**.

If you have questions or comments about this series, or would like to see other use cases, feel free to contact us through twitter at **@identitymind** or send us an email to **evangelist@identitymind.com**.