

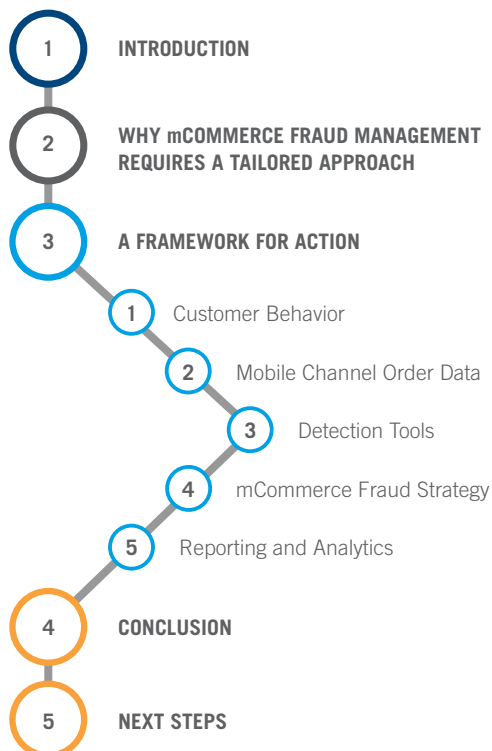
A FRAMEWORK TO HELP MANAGE mCOMMERCE FRAUD



OVERVIEW

AS mCOMMERCE GROWS IN VOLUME AND VALUE, THE WAY YOU MANAGE FRAUD IN THE MOBILE CHANNEL BECOMES CRITICAL TO SUCCESS

CONTENTS



INTRODUCTION

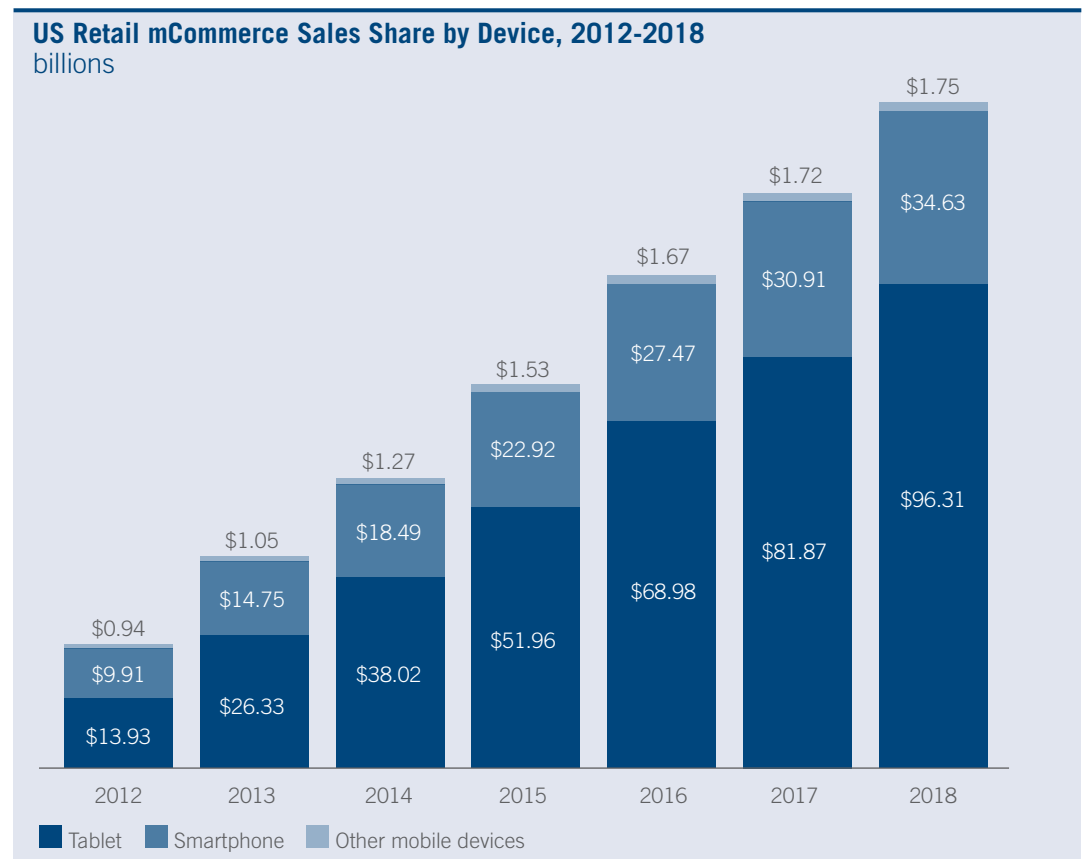
As CyberSource engages with businesses about their ambitions for digital commerce growth, one of the messages consistently heard is that the future is mobile. Whatever their size and industry, these businesses understandably want to take advantage of the continuing growth of smartphones and tablet penetration, and their use by consumers to purchase goods and services.

As companies embrace the mobile channel, many don't distinguish between eCommerce and mCommerce (or the mobile channel) from a fraud management perspective. The same fraud management strategies and tools are used for both, and it's common to find that the mobile channel is not tracked separately.

While there are many similarities between eCommerce and mCommerce, there are also important differences that are particularly relevant to fraud management. If these differences aren't anticipated and planned for, organizations may experience higher rates of fraud in the mobile channel than they want to, or reject or review too many genuine mCommerce transactions (or both).

Many companies are today successfully managing mCommerce fraud to levels that are the same or lower than their eCommerce fraud rates¹, and this is a key success factor in helping them fulfil their mobile channel growth plans with confidence.

This paper provides a framework for thinking through these differences, and offers advice and strategies to help you manage mobile fraud effectively and improve the mobile experience of genuine customers.



Source: eMarketer, April 2014.

Note: includes products or services order by using the internet via mobile devices, regardless of the method of payment or fulfillment; excludes travel and event tickets.

¹CyberSource 2016 Online Fraud Management Benchmarks Report – North America Edition.

WHY mCOMMERCE FRAUD MANAGEMENT REQUIRES A TAILORED APPROACH



DEFINING mCOMMERCE

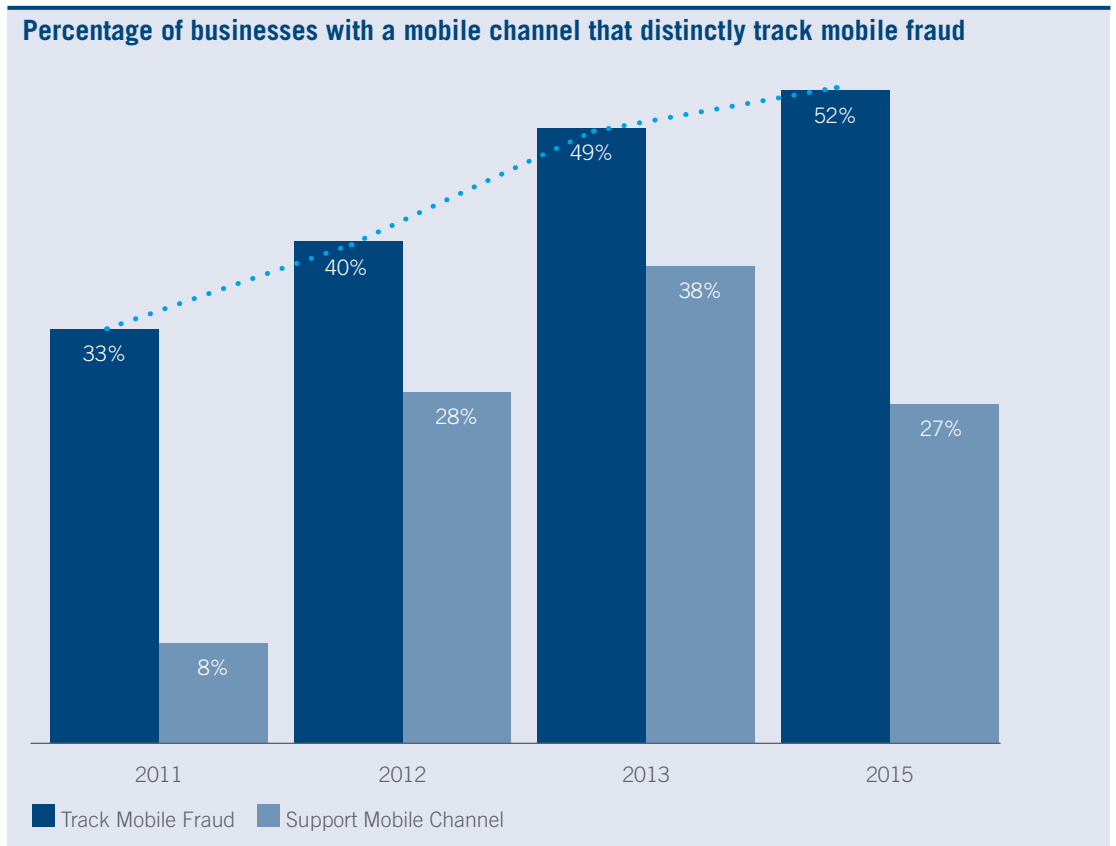
For the purposes of this paper, mCommerce refers to an online purchase originating from a consumer-owned mobile device such as a smartphone, tablet, Kindle or similar device, using a mobile browser or app. It doesn't refer to in-store mobile payments or mPOS.

Laptops are not included in our definition. Although portable, their pattern of use is much more similar to a desktop PC than to other mobile devices.

It's the device – the form factor or the operating system being run – that is the key element in distinguishing mCommerce from eCommerce for fraud management purposes. Mobile access may ultimately be via cellular tower or Wi-Fi, and this may affect some of the data associated with a transaction; but in both cases it should be treated as a mobile transaction when managing fraud (for reasons that this paper explores).

Most businesses appreciate the need to tailor their eCommerce customer interface for mobile sites and apps. For example, standard full-screen website designs may be hard to navigate on a much smaller screen and this is why mobile-enabled sites are provided.

When it comes to fraud management, very few businesses are distinguishing mCommerce from eCommerce. The 2016 CyberSource Online Fraud Management Benchmarks study found that only half of businesses with a mobile channel even track mobile fraud separately.



Source: CyberSource 2016 Online Fraud Management Benchmarks Report – North America Edition.

When businesses don't adapt their fraud management strategy to their mobile channel – or even track mobile orders separately – they may become vulnerable in two significant ways:

The risk of higher mobile fraud rates

A physical goods retailer asked CyberSource for assistance when they discovered that while mCommerce accounted for around 10% of their transactions, it represented 20% of chargebacks.

This is not an unusual experience. Fraudsters are aware that businesses can be slow to adapt to a new channel, and they're quick to take advantage. They may notice before you do that your existing fraud rules aren't fully suited to the mobile channel, and quickly exploit the differences between mCommerce and eCommerce to slip through your defenses.

The risk of blocking genuine customers

The second risk of not adapting fraud management to the mobile channel is that too many genuine mCommerce orders may get rejected or identified for review.

Often this is the larger problem for businesses. The last thing you need when you're trying to grow the mobile channel is for your customers to have a less-than-ideal mCommerce experience. Higher rejection or review rates can also translate into a loss of revenue or higher fraud management costs, neither of which is generally acceptable.

What to do?

How can fraud rules be both too permissive for fraudsters and too blunt for genuine customers? The rest of this paper explores why and how this is the case, and what strategies can be implemented to help manage mobile fraud effectively and improve your chances of success with your mobile channel.



STRATEGIES FOR SUCCESS

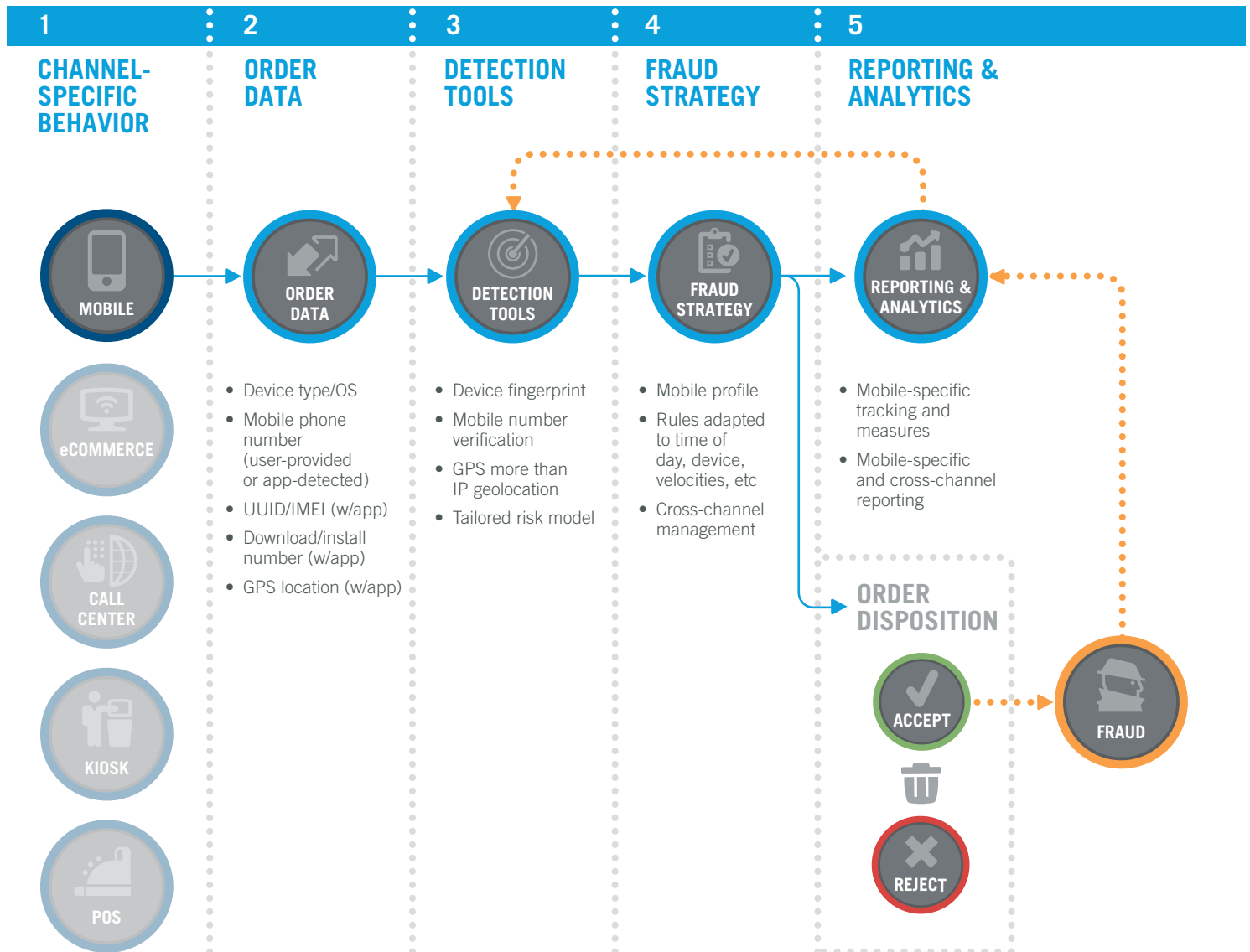
When businesses discover that their mobile fraud rate is higher than they'd like, their first instinct may be to react quickly, with 'blunt' rules that cause them to review or reject more mobile orders. This approach may enable more fraudulent orders to be identified, but there's a significant risk of catching genuine orders in the same net.

An effective strategy is to err on the side of genuine customers, accept a higher rate of fraud in the short term, and work quickly to identify chargeback patterns and mobile-specific rules that can more effectively distinguish fraudulent from genuine mobile behavior.

A GOOD STRATEGY IS TO ACCEPT A HIGHER RATE OF FRAUD IN THE SHORT TERM VIA MOBILE, AND WORK TO IDENTIFY CHARGEBACK PATTERNS AND MOBILE-SPECIFIC RULES.

A FRAMEWORK FOR ACTION

The framework below provides an example of a process-based approach to work through the differences between mCommerce and eCommerce for fraud management. Working through the process step-by-step can help you understand the implications of the mobile channel for fraud management, and equip you to decide on the best course of action for your organization.





1. CUSTOMER BEHAVIOR

Understanding the differences between anomalous and normal behavior is the foundation of any effective fraud management strategy.

It's therefore important to recognize that normal customer behavior on a mobile device is often different from normal customer behavior on a PC (a laptop or desktop computer). eCommerce fraud detection rules are designed for typical PC behavior. Whenever mobile behavior differs, these rules may treat perfectly normal behavior as anomalous.

Some mobile behavioral differences:

Number of mobile devices used

It's common in many countries for people to use multiple mobile devices within a short timeframe: switching between their own tablet and phone, for example, or using their tablet and then their spouse's. If a rule treats multiple devices logging into an account as suspicious behavior, it may flag what is increasingly normal behavior in the mobile channel.

Transacting while on the move

It's feasible for somebody purchasing through a mobile device to be doing so while actually in motion: in a car or train, for example. As they move, they become connected via different cellular towers, and this can cause problems for rules based on IP geolocation criteria.

Even when mobile users are stationary, they may be anywhere in the world. The IP address that is detected will depend on specific networks traversed and the approaches taken by different network providers; none of which is transparent. The very mobility of mobile devices, much greater than for laptops, makes IP geolocation less useful and potentially exploitable by fraudsters, as well as raising the risk of potentially identifying genuine orders as fraudulent.

Provision of mobile number

Many businesses ask customers to provide a phone number as part of their identity verification. They may use third-party records to check validity, or check their own records for a previously provided number. Increasingly, but especially if the device being used to place the order is a mobile, customers give their mobile number rather than the landline number that third-party or internal records are more likely to have. The mismatch between numbers could raise a red flag if not anticipated.

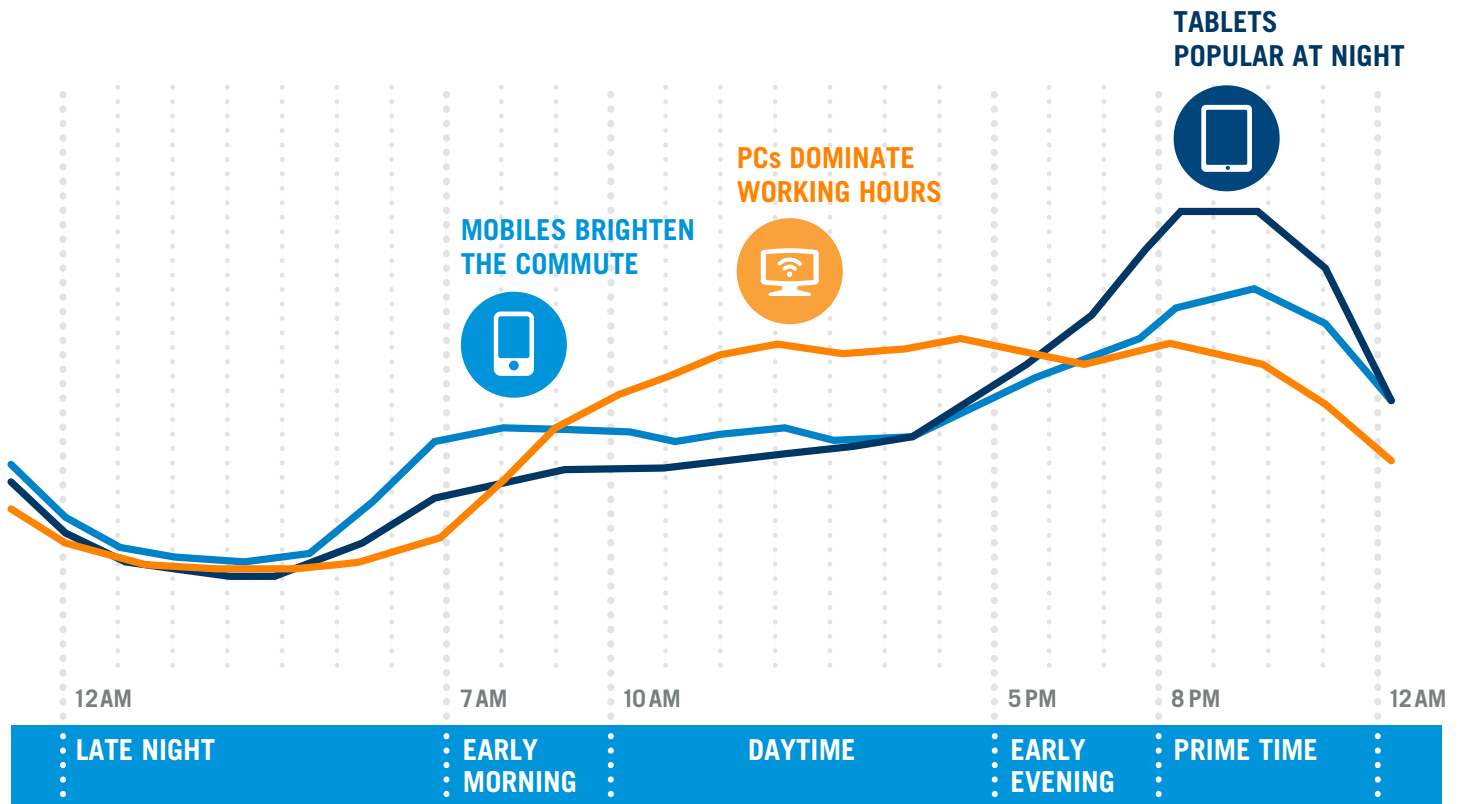
IT'S IMPORTANT TO RECOGNIZE THAT NORMAL CUSTOMER BEHAVIOR ON A MOBILE DEVICE IS DIFFERENT FROM NORMAL CUSTOMER BEHAVIOR ON A PC (A LAPTOP OR DESKTOP COMPUTER).

Time of day

It's common to have rules that recognize certain times of the day as more risky than others. A rule may reflect the possibility that an order placed from a local IP address late at night really emanates from a different time zone (i.e., a different country). For example, Web purchases via a PC usually dips after around 8pm but mobile devices generally see their highest use at night.²

At home mobile devices may connect in exactly the same way as the PC, but they still have distinct patterns of use. These differences need to be recognized and accounted for, to deal effectively with mCommerce from a fraud management perspective.

Share of device page traffic on a typical workday



Source: Ooyala Global Video Index, Q3 2014 <http://bit.ly/1KxEVkb>.

²Ooyala Global Video Index, Q3 2014 <http://bit.ly/1KxEVkb>



2. MOBILE CHANNEL ORDER DATA

Along with understanding what constitutes normal and anomalous behavior, effective fraud management depends on data: as much as can be gathered, for as many relevant variables as possible, collected in consistent ways that facilitate comparison and correlation.

Whether data is being used to identify the channel a customer is using, the time of day they're doing so, where and who they are, or what they are buying, all of the information captured about an order becomes an input to the tools and rules of fraud management. The more relevant data there is, the more can be done to distinguish genuine from fraudulent transactions.

Considerations when capturing device type

One of the most obvious way to identify transactions as mobile in order to treat them differently from non-mobile orders is to capture the device type.

This can be done in more than one way. Examples include capturing the fact that an order has come through a mobile website or app; or capturing and analyzing the device fingerprint. If the aim is solely to identify a transaction as mobile, there's no need to capture anything more specific than 'mobile device'. But there's good reason to get more specific and use device fingerprinting to capture whether a device is, for example, an iPhone or an Android phone.



What is a device fingerprint?

A device (or machine or browser) fingerprint is a string of information about a computing device, used for the purpose of identifying the device. It may include information such as the operating system, browser configuration (for example, are cookies turned on or off), TCP/IP configuration, wireless settings, and clock skew. Depending on the tools used to collect the device fingerprint, it may even include attributes such as the device MAC address or hardware serial numbers. The principle is that, as long as a sufficient number of relatively stable attributes is collected, each device should have a unique combination.

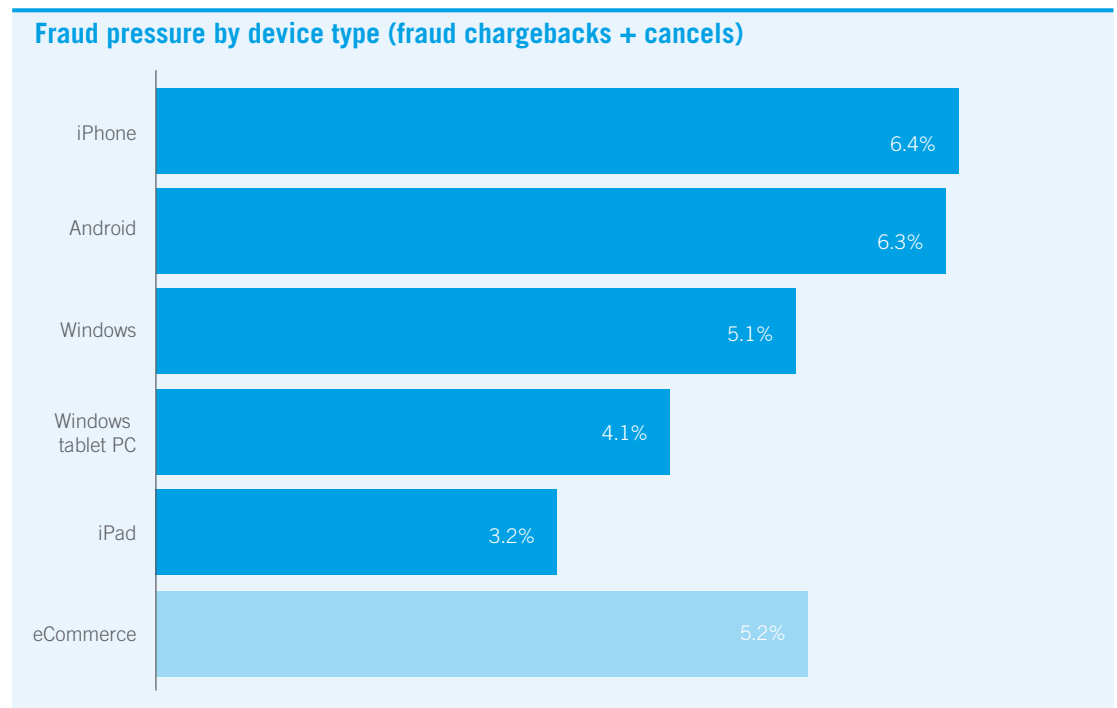
THE MORE RELEVANT DATA THERE IS, THE MORE CAN BE DONE TO DISTINGUISH GENUINE FROM FRAUDULENT TRANSACTIONS.

Why specifics matter

One reason to capture more specific data is that different device types can be associated with different rates of fraud pressure, as the figure below shows. The low incidence of fraud for tablets probably reflects the hybrid nature of tablets between PC and phone. People may use their tablets as a (more mobile) PC, making them a better fit to eCommerce fraud detection strategies, with iPads also benefiting from the relative scarcity of successful attacks on Apple devices.

The fraud pressure rates shown in the figure combine fraud that has been successfully perpetrated (chargebacks) with fraud that has been attempted but successfully prevented (cancels/rejects minus false positives). By reflecting all attempts at fraud, both successful and unsuccessful, we can get a better indicator of fraud risk – the likelihood of fraud happening if nothing is done to prevent it.

Knowledge of these different risk profiles can be used within fraud scoring and rule creation; but only if enough data is captured to distinguish, for example, iPhones from iPads, and Windows from Android phones.



Source: Decision Manager, January – June 2015 Global credit card transactions where device identified.

Note: The numbers are high because they combine fraud that has been successfully perpetrated (chargebacks) with fraud that has been attempted but successfully prevented (cancels/rejects minus false positives).

Variation in data availability

Most of the information captured for mCommerce orders will be the same types of data captured for eCommerce, but the specifics may differ. As seen in a previous example, for instance, people are more likely to provide a mobile telephone number than a landline when using a mobile phone.

Sometimes additional data can be extracted from a mobile transaction than from an eCommerce transaction; sometimes less.

For example:

- iPads and iPhones provide a much diluted device fingerprint because of how ‘locked down’ the Apple OS is and the very basic nature of the information provided by popular browsers such as Safari and Opera.
- Conversely, the Samsung mobile browser provides quite specific details. By capturing additional details when the data is available, trends can be spotted that enable more sophisticated fraud rules to be implemented.

Examples of device fingerprints

Mozilla/5.0 (**iPad**; CPU OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML

Mozilla/5.0 (**iPhone**; CPU iPhone OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML

Mozilla/5.0 (Linux; Android 4.4.2; **es-es**; **SAMSUNG GT-I9505-ORANGE Build/KOT49H**) AppleWebKit/537.36 (KHTML

.... Indicates Spanish user

.... Indicates Samsung Galaxy S4 Black Edition

MOST OF THE INFORMATION CAPTURED FOR mCOMMERCE ORDERS WILL BE THE SAME TYPES OF DATA CAPTURED FOR eCOMMERCE, BUT THE SPECIFICS MAY DIFFER.

Native mobile apps are the most obvious source of additional data for mobile transactions. Because an app can be specifically designed to capture additional data (see the ‘strategies for success’ below for an important consideration here). Just a few key pieces of data captured from a native app can help to improve mobile fraud management:

- **Download/install/activation IDs.** It’s standard for app developers to include the generation of one or more proprietary unique identifiers. Each download of an app will almost certainly have an associated ID, and an ID may also be generated when the app is first activated on the device. These can be used to track multiple identities associated with a single download instance, which might suggest a fraudster trying different stolen identity or payment information.
- **Universally unique identifiers (UUIDs).** All of the devices used by your customers should have at least one unique device identifier. The value of capturing a device UUID is that it remains the same if, for example, a fraudster deletes an app and downloads it again in an attempt to associate a new payment ID with a different download ID. One company that we work with manages different versions of its app: its own and several differently branded versions used by partners. The company uses device UUIDs to help track fraudsters trying one app version after another in an attempt to complete a transaction.

There’s no problem with the capture of UUIDs from Android phones, but Apple is making a sustained effort to stop this kind of device information being collected, and will reject apps from its app store if they are designed to collect information such as the unique device identifier (UDID) that all Apple devices have. This removes an important tool from the fraud management toolkit, but this is perhaps balanced by the fact that Apple’s greater control over its OS and app store seems to make its devices less subject to fraud pressure (as things currently stand).

Different types of device UUIDs	
The world of device identifiers is a maze of acronyms. The most common are:	
IMEI	International mobile station equipment identity
MEID	Mobile equipment ID
UDID	Apple’s unique device identifier, a value calculated from a number of device-related variables, including the IMEI/MEID or another unique identifier that some Apple devices have, the ECID.

- **Mobile phone number.** This can’t always be captured – it depends on the platform – but if captured it can be used in combination with the other data points to track the use of different SIM cards in different devices and make decisions about the likelihood of fraud being perpetrated. It can also be used to look for a match if customers are asked to provide a phone number at checkout (or have provided one before when registering).
- **GPS data.** If an app can use GPS and the device has it switched on, this can be used instead of IP geolocation in rules that use the buyer’s location as one of the inputs to help make fraud-related decisions. However, genuine customers may use their mobile devices anywhere in the world, and may not appreciate fraud rules that don’t take this into account. This is why it’s common for payment card providers to ask cardholders to tell them when they may be using their card abroad.

How to capture this data

The most reliable way to capture much of the device and usage-related data that is useful for fraud management is through the use of an established mobile device management (MDM) application or service. Many, including Apple's MDM, AirWatch, MobileIron, IBM's MaaS360 and SOTI.

These solutions specialize in accessing information from mobile platforms efficiently and securely, and they are better placed than most app developers to keep up with the pace of change in mobile management technology. The other half of the equation is then to have a fraud management tool that can access the relevant data gathered by your MDM platform.



STRATEGIES FOR SUCCESS

Consider capturing as much data as possible, even if it's not immediately useful. If a future strategy requires the use of a new variable, the strategy will be easier to implement if the relevant variable is already being captured.

The value of data capture should be balanced with caution when capturing data via an app, to avoid legal and privacy concerns. Consumer unease about the data that apps collect is already an issue, and it will likely increase with the growth of the mobile channel, as early adopters give way to more conservative users. The more you can cater to privacy concerns while still capturing enough to provide a good level of protection, the more successful you're likely to be with app adoption.

BROWSER VS APP: IS ONE BETTER?

Companies often ask whether they should implement mCommerce through a native app; or through a mobile-friendly site (or hybrid app: a downloaded shortcut to a mobile-friendly site, with the browser elements hidden from the user) – or both. The answer depends on a multitude of business-specific considerations, but it's worth noting some of the factors besides fraud management that are relevant to the decision:

	Browser	App
Pros	Customer experience <ul style="list-style-type: none">Catching up with app experience through advancements in HTML5No download or updates required IT management <ul style="list-style-type: none">Easier server-side updates	Customer experience <ul style="list-style-type: none">User-friendlyGreat for repeat purchase (accounts)Ideal for certain verticals (e.g. travel) Fraud management <ul style="list-style-type: none">Collect more customized data (e.g. download/install ID; UUID/IMEI; phone number)GPS potential
Cons	Fraud management <ul style="list-style-type: none">Variable device and device fingerprint informationLess useful IP geolocationBrowser strings can be spoofed	Customer experience <ul style="list-style-type: none">App and app update fatiguePrivacy concerns IT management <ul style="list-style-type: none">More expensive to update and coordinate Fraud management <ul style="list-style-type: none">Exploitable security flaws (e.g. pwords stored in plain text, unsecured persistent login)



3. DETECTION TOOLS

Similar fraud detection tools will typically be used for both mCommerce and eCommerce, but their relative importance may differ.

Geolocation detection

As already noted, IP geolocation may be less useful in the mobile channel, but the mobile-specific tool of GPS-based geolocation may be available to use instead.

3-D Secure

3-D Secure may be less useful in the mobile channel, because traditional implementations of Verified by Visa, MasterCard SecureCode and other 3-D Secure schemes haven't been optimized for the smaller form factor of mobile devices. Customers may also be less tolerant of the extra step in a mobile checkout scenario.

Options for mobile implementation will no doubt improve – for example, by enabling it to be implemented within the checkout page, and giving businesses more control over which transactions warrant the 3-D Secure step.

Phone number verification

Phone number verification may be useful in the mobile channel, if you are able to capture and validate mobile phone numbers. Not only can the mobile number be a very important piece of data for establishing customer identity, but once stored on record it can also be used to minimize manual review by employing automated SMS validation on suspect orders.

Device fingerprinting

It's common to hear that device fingerprinting is less useful in the mobile channel, on the basis that mobile device fingerprints are more limited than those typically available from PCs. However, when device fingerprinting is considered as one tool among many, especially when combined with an understanding of the mobile environment and behaviors, it can be a very important tool.

Mobile devices are personal items, almost always in the possession of the owner or someone they trust, and unlikely to be used without the owner's knowledge or permission. While mobile botnets do exist, this kind of compromise is still rare in the mobile space, and this means that there's a likelihood that a device fingerprint associated with prior genuine transactions can be trusted when encountered again. Fraud management is as much about creating a positive customer experience as it is about preventing fraud, so the ability of device fingerprinting to help identify returning customers makes it valuable, especially in the mobile space where IP geolocation is less useful.



STRATEGIES FOR SUCCESS

One of the most important tools in the fraud detection kit is statistical risk modelling. Creating and applying a risk model tailored specifically for mobile transactions enables a more accurate risk score to be generated for mobile transactions, reflecting mobile-specific data and trends.



4. mCOMMERCE FRAUD STRATEGY

All of the differences in behavior, data and tools associated with the mobile channel lead logically to differences in fraud rules – especially with the objective of minimizing automatic review or rejection of genuine mCommerce orders.

The examples below illustrate the point:

- Rule A for mCommerce recognizes that it's unusual for orders placed on mobile devices to contain many different items. This would be an inappropriate rule for eCommerce because it's common for PC users to take the time to order multiple items together.
- The reason that rule A for eCommerce doesn't have an equivalent for mCommerce is that it looks for a mismatch between proxy IP country and true IP country: an internet routing irregularity that wouldn't be so straightforwardly applicable to the mobile channel because of the issues with IP geolocation.
- Rule B for mCommerce reflects the fact that – in the country where this rule is being applied – it's atypical for a mobile device to be used by more than one person, who is unlikely to have more than a few emails. By contrast, the number of users and emails associated with PCs shows much more variability, resulting in a different sensitivity for the rule and a different threshold of fraud risk score for invoking the rule.

Examples of eCommerce and mCommerce rules that would lead to an order being manually reviewed

mCommerce	eCommerce
<div><div>• AFS = • fraud risk score</div><div>• ITC = • different items in cart</div><div>A. AFS >30, ITC >5</div><div>B. AFS >40, EMD >2</div><div>• EMD = • emails for this device</div></div>	<div><div>• MM-IPC = mismatch • between IP and country</div><div>A. AFS >40, MM-IPC</div><div>B. AFS >45, EMD >5</div></div>

The fundamentals stay the same

As with eCommerce, the rules created for mCommerce will depend on the data that can be captured, the behavioral patterns and fraud trends that are understood to be relevant, and also the level of sophistication that suits your organization's requirements and risk profile.

It's not necessary to achieve high sophistication immediately. Here are some straightforward early steps:

- Start tracking mobile transactions. Measuring mobile chargeback, rejection and review rates will enable informed decisions to be made about when and how to act.
- Create a distinct mobile profile, even if at first the rules applied are an exact copy of existing eCommerce rules.
- Start capturing the device type and operating system, even if no rules are immediately implemented based on the differences in fraud pressure between different devices.

As mCommerce grows in value and the mobile channel becomes more familiar to your business, increasing sophistication of analysis and detection will naturally follow. It can be helpful to have mobile specialists within the order review team, who can help to spot patterns that can be fed back into rule creation for the mobile channel. Non-specialist reviewers may need training to understand and act on the differences between mCommerce and eCommerce.

Understanding the bigger picture

Another fundamental of fraud management is the importance of keeping track of fraud across all of your channels. Fraudsters will move between channels as they try to exploit both eCommerce and mCommerce. Important as it is to segment these channels, it's equally important to be able to integrate them for analysis and to spot activity and patterns in one channel that affect actions in another.



STRATEGIES FOR SUCCESS

If your organization chooses the app route for mCommerce, a key to successful fraud management is to insist that app security be taken seriously. It's not uncommon for app development to happen quickly and to focus almost exclusively on the user experience – with security being an unfortunate casualty. Passwords may be stored as plain text, persistent login may be implemented without sufficient protection against session hijacking, or there may be other vulnerabilities that can be exploited. Avoiding or mitigating app security flaws in the development stage is a vital ingredient in the fraud management mix.

AS mCOMMERCE GROWS IN VALUE AND THE MOBILE CHANNEL BECOMES MORE FAMILIAR TO YOUR BUSINESS, INCREASING SOPHISTICATION OF ANALYSIS AND DETECTION WILL NATURALLY FOLLOW.



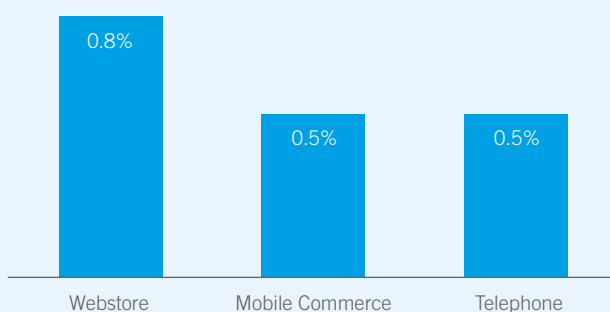
5. REPORTING AND ANALYTICS

You can't manage what you can't measure.

Companies that aren't tracking mobile fraud usually guess that fraud rates are higher for mCommerce than for eCommerce: the general perception is that 'mobile is riskier'. Businesses that actively manage mobile fraud can achieve

fraud rates that are similar to their rates for other channels (see figure). In our experience, above-average mobile fraud rates are usually a sign that a mobile-specific fraud strategy either isn't in place, or needs to be fine-tuned.

Fraud rate for different order channels



Source: CyberSource 2016 Online Fraud Management Benchmarks Report – North America Edition.

Once a mCommerce fraud management strategy is in place, it's even more important to monitor, measure, analyze and fine-tune than it is for more established channels. The mobile space is still relatively unfamiliar, and likely to change in many ways as mCommerce grows and matures. There's still a lot to learn about fraudster strategies and exploits, which are also likely to evolve very rapidly

in these early days. As new customers adopt the mobile channel, how might behavior patterns change? A pattern that's true today may not be true tomorrow.

It's important to capture as much data as you reasonably can, because any data element might prove significant for managing mobile fraud more effectively in the future.



STRATEGIES FOR SUCCESS

Passive-mode testing of rules can be extremely valuable, but even more so for a new channel in which there is limited prior experience to help anticipate the effects of a proposed new or amended rule. With passive testing, the results of applying a potential mCommerce rule to actual transactions can be seen without applying it live, enabling its effectiveness to be judged before implementation.

If you also have the ability to do this on historical data – which we call 'transaction replay' – it becomes even more powerful. It means you can see the effect of a potential rule on specific transaction types or periods of interest, without having to wait for those transaction types or periods to occur in future.

CONCLUSION

Effective fraud management is one of the critical success factors for eCommerce growth. It's no different for mCommerce.

The ability to understand how consumer behavior differs when using mobile devices; to capture data that is relevant to the mobile channel and implement appropriate fraud management tools and rules; to track and analyze mCommerce chargeback, rejection and review rates and fine-tune your strategy in response – all have clear implications for the experience that both customers and fraudsters will have when they interact with you through the mobile channel.

Whether by yourself or with the help of a fraud management solution or service provider, working your way through the framework provided – taking advice as necessary and doing the appropriate research to delve deeper – may help you create an appropriate mCommerce fraud strategy for your organization and develop it over time. It can help you acquire the knowledge and tools to achieve the double goal of welcoming genuine customers and turning fraudsters away.

NEXT STEPS

To discuss your situation and find out how CyberSource can help you optimize fraud management operations for mobile payments and across channels, please contact us at any one of our global locations.

CyberSource's Decision Manager gives you the tools to successfully manage fraud as your organization embraces new payment channels and geographies.

Accept more orders, with less fraud

One connection to CyberSource gives you everything you need to manage fraud with confidence. With specialized fraud models optimized for the mobile channel, you can accept orders from any channel while keeping fraud under control. Detailed fraud insights from the World's Largest Fraud Detection Radar and our in-country specialists also help you manage fraud on a global scale. Decision Manager Replay helps you ensure that new rules are as effective as possible through faster and better testing.

Reduce the cost and complexity of fraud operations

With CyberSource you gain tools to accurately sort and highlight orders for review, and an extensive support network of analysts and review teams to help you spend less time manually reviewing and analyzing data. You can also use rules-based authentication to reduce fraud liability and costs without harming your customer's experience with you.

Keep customer accounts safe

By monitoring login activity and customer accounts, you can keep your customers' accounts safe from fraudsters using CyberSource Advanced Account Takeover Screening. By connecting to CyberSource, you'll be able to confidently manage fraud wherever your business takes you.