

COLUMNS

## 3 tips to protect against mobile commerce fraud

June 9, 2015



*Tom Donlea is director of ecommerce at Whitepages*

By **Tom Donlea**

By now, all online retailers know how vital mobile commerce is to their business' success. That likely has something or everything to do with the fact that mobile sales grew 47 percent year over year during the second quarter of 2014.

Even though merchants have upped their mobile commerce game, major obstacles remain. The first is satisfying the average consumer's worry that mobile commerce is not as safe as other channels. And the second relates to the first: Retailers need better ways to fight mobile commerce fraud.

Mobile commerce is without a doubt the riskiest method of sales.

In 2014, merchants experienced nearly double the fraud rate in mobile commerce versus ecommerce. No doubt this is due to high numbers of data breaches and the accessibility of so much consumer contact information.

So what can merchants do?

The answer is simpler than you think: Build your knowledge on how mobile commerce fraud occurs and admit you need additional tools for your ecommerce fraud platform that will appropriately defend against mobile fraud.

Here are three tips for you to improve your mobile fraud review and speed more good orders to clear:

1. Know your entry point

In mobile commerce, there are three different paths that a consumer can take to buy from you. They are:

Desktop Web site via a mobile device

Mobile-optimized Web site

Mobile application

Merchants have always been savvy at sniffing out fraud, but it is much harder to do if you do not know which of your channels let the bad order through.

Florida-based consultancy The Fraud Practice found that only half of the retailers they surveyed had the ability to track which channel individual orders originate from, and yet more than 60 percent answered that it was important to know whether or not the transaction was mobile fraud.

Using mobile apps is the most secure way to transact via the mobile medium, but since consumers demand options, not every ecommerce operation can offer this entry point. It is important to find a fraud platform that tracks order

origination so you can take steps to optimize against bad orders.

## 2. Watch out for digital gift cards

The purchasing of digital gift cards via mobile has the highest likelihood for fraud.

In fact, it is the most common form of fraud for any customer-not-present transaction.

The reason why it is preferred by fraudsters is that it is a hassle-free way to use a stolen credit card and get 60 percent to 70 percent of the value by reselling it in an online marketplace or pawnshop.

You need to perform thorough identity verification before approving these highly liquid transactions.

## 3. Dig deeper into guest transactions

Are all consumers who attempt to check out without establishing a user account fraudsters?

The answer depends somewhat on your business, but when this does happen you should strongly consider adding at least moderate friction during the checkout process.

Asking them to verify their mobile phone number is an easy step that can protect against fraud and chargebacks.

WHAT ALL OF these tips have in common is the need for mobile commerce retailers to collect more data.

With additional consumer information, you can achieve the level of analysis that is key for separating the good orders from the bad.

Get your business a fraud platform that performs accurate and insightful identity verification for every possible point of mobile sale.

You will find that you will improve your speed-to-clear and spend more of your review time on the orders that are actually suspicious.

By boosting your identity verification processes, you will reduce mobile fraud and speed more good orders to clear. This leads to the rocket-like result that every retailer likes: a revenue boost.

*Tom Donlea is director of ecommerce at [Whitepages](#), Seattle. Reach him at [tdonlea@whitepages.com](mailto:tdonlea@whitepages.com).*