Luxury Daily®

The News and Intelligence You Need on Luxury

COLUMNS

Why your mobile behavior is a magnet for fraud

November 1, 2011

By Alisdair Faulkner

Mobile is more than technology. For many consumers, mobile is a way of life – a real-time response tool they can use to buy everything from movie tickets to luxury automobiles.

In 2010, the top mobile purchases on eBay were vehicles. Some consumers spent six figures on new wheels, completing the sale from a convenient and portable mobile device platform.

But consumers and retailers are not the only ones noticing that mobile commerce is poised for explosive growth. Cyber-criminals are way ahead of the game. And many of them have already started to mine the mobile universe for easy profits.

Risky behavior

Mobile technology is chock-full of features and behavior that are attractive to fraudsters.

For example, app stores are essentially fraud superstores, providing a delivery platform for dubious apps that embed malware in user devices.

Since most mobile users do not install anti-spy or anti-virus solutions, fraudsters use app stores, text messaging and device and mobile gateway vulnerabilities to harvest online account credentials and personal data.

When it comes to fraud detection, retailers find that traditional tactics do not cut it in the mobile realm.

Since mobile users typically connect through an assortment of Wi-Fi networks and 3G gateways, threat monitoring based on IP addresses is not an option.

It is also difficult for retailers to authenticate users based on digital device fingerprints, in comparison to PCs that have more unique profiles.

Fingerprints that rely on cookies or Flash technology are not available on some mobile platforms such as iPhones and mobile devices can be easily lost or stolen.

But from a fraud prevention perspective, the most disturbing mobile behavior is also mobile's most important benefit: instant access.

Consumers demand real-time response capabilities – the ability to achieve anytime, anywhere connections to retailers via their mobile devices.

Retailers accommodate the expectations of mobile consumers with automated purchasing tools – the same automated purchasing tools fraudsters hijack to secure and distribute merchandise to locations across the globe.

Fraud prevention strategies

Mobile commerce requires real-time purchasing capabilities to be convenient. For retailers, this means adapting fraud platforms to accommodate real-time analysis and to address threats created by mobile behavior.

• Review existing transactions and fraud rules. Do you know what percentage of transactions come from mobile devices today? Start by reviewing your existing transaction patterns, then do a thorough review of existing business rules to make sure good mobile transactions are not being rejected or caught up in review queues by outdated rules.

• Centralize intelligence. Fraud intelligence needs to be centralized across all Web and mobile applications. If done effectively, the benefits of centralization will be greater fraud detection capabilities and reduced fraud prevention costs for retailers.

• Webify mobile transactions. While mobile apps provide great interactivity, you should redirect all transactions to a mobile Web interface and leverage your existing PCI compliance and Web-based payment workflow. Retailers would not store sensitive information on a PC, and same goes for mobile devices.

• Layer. Layered security is critical in mobile fraud prevention. It is foolish to think that fraudsters will not eventually crack a single layer of security. The creation of multiple security layers reduces the risk associated with the breach of a single security measure, making it more difficult for unauthorized users to access account credentials and other sensitive data.

· Focus on location. Mobile GPS and location tracking is emerging as a new method of identifying user behavior signatures to verify and authenticate transactions and account access. However, location tracking is a potential privacy time-bomb, so retailers will need to be transparent and get explicit consumer consent.

BETTER MOBILE security will require modification to existing device identity and behavior-based fraud filters.

For retailers, the trick will be striking the right balance between consumer convenience and improved security in a mobile environment that is increasingly characterized by privacy concerns.

Alisdair Faulkner is chief products officer of ThreatMetrix, Los Altos, CA. Reach him at afaulkner@threatmetrix.com.