Preventing Transaction Fraud with Location-Based Services (LBS)

David Allen, CTO, Locaid Technologies

A recent Federal Bureau of Investigation report stated that "identity theft has emerged as a dominant and pervasive financial crime that exposes individuals and businesses to significant losses and undermines the credibility and operation of the entire U.S. financial system." In addition, the National Strategy for Trusted Identities in Cyberspace (NSTIC) estimates that 11.7 million Americans were victims of some kind of identity theft over a two-year period. As more and more people use mobile phones for commerce, banking, healthcare, and other highly confidential transactions, the risk for identity fraud increases because mobile phones are widely exposed to security threats and spoofing. This paper will examine fraud risks and how mobile phones and wireless networks can be used to prevent fraud and protect against identity theft during traditional credit/debit card and mobile banking transactions.

Location platforms enable financial institutions to connect directly to wireless carrier networks and obtain mobile subscriber location data. Under a privacy-protected, permission-based location platform, banks can determine a customer's mobile device location at the time of a transaction. By comparing device location to transaction point of sale data, one can make a determination if the transaction is potentially fraudulent.

By connecting directly to the carrier location networks via a location aggregator, financial institutions are accessing real-time network location, not device-dependent application location. Application location, like the kind used in social networking apps such as Foursquare "check-ins" and Facebook Places, can be spoofed in a matter of minutes.

Besides mobile banking applications that enable a user to access bank account information via a smartphone application, a new technology has emerged in the mobile space that industry experts predict will not only be the next generation of the alternative payments industry, but will completely replace plastic credit and debit cards altogether.

Near-field communication (NFC) is a wireless technology that allows short-range communication between electronic devices. In terms of mobile payments, NFC will enable mobile users to make contactless transactions in brick-and-mortar stores with a simple RFID connection. In order for the technology to work, an NFC chip must be physically embedded in a phone and a store's POS system must be updated to accept it. The mobile industry predicts that the number of mobile devices with embedded NFC technology will likely hit 200 million by the end of 2012. Speculation of NFC inclusion in the iPhone 5, along with chatter about the iWallet, Google Wallet, and other similar mobile payment applications, all indicate that NFC is poised for explosive growth in the coming months. In addition, consumer spending via smartphones has grown exponentially since 2010.

One looming problem for NFC mobile transactions is fraud, largely because many people still view their phone as a communication device rather than a personal device meant to be secured.

Many view NFC for mobile payments as a way to curb identity fraud associated with stolen credit cards and ATM skimming, since verifying physical presence is thought to reduce fraud. However, like with other physical location technologies sourced solely on the device itself, the location of these chips can potentially be spoofed, thus eliminating security benefits. Conversely, network-based location *can* authenticate physical presence, and acts as a third-party verifier for near-field communications and traditional credit/debit card transactions when used for mobile banking.

To use location as a third-party verifier for NFC and mobile payments, a merchant POS location is compared to a mobile phone location and assigned an algorithmic fraud identification score based on the proximity of the two locations. Based on the score, the payment will either be accepted, or will be sent as a notification to the financial provider to determine whether a fraudulent action has or is about to occur. Not only does this reduce fraudulent charges to a consumer's account, but reduces the cost to a bank that would've had to conduct a false-positive investigation. Each time a false positive occurs, it costs a bank between $25 and $40 per transaction to cover administration and time. Comparatively, using location to verify a false positive, costs the bank a nickel.

With secure network-based location, consumers benefit from increased personal and financial security, while bank benefits include a reduction in false positive cases, case management loads and customer service interventions. In terms of ATM skimming, location helps qualify transactions as fraudulent during the transaction, focuses resources on problem areas and improves ROI on fraud pursuits.

In conclusion, the mobile industry needs to apply location verification to both mobile payments powered by NFC, and traditional credit and debit card transactions, to reduce bank costs, authenticate location, and provide peace of mind to consumers.