Yodo’s Mobile Money system

(Security & Compliance Issues)

The variety and features of mobile payments are highly variable and constantly evolving. Mobile money which essentially relies upon a person’s mobile phone for access, like the phone itself often crosses numerous legal and geographic boundaries being as its name implies highly mobile. FinCen in the United States and FinTrac its Canadian equivalent have recently provided guidelines and rules for Money Service Businesses (MSB) and in particular for Pre-Paid Access to which Yodo’s Mobile Money process may be subjected.

Yodo’s product uses cash (which is anonymous), as its core payment engine and as such individual users may remain anonymous. Some of the submissions by the incumbent MSB and therefore some of the regulation being postulated by national authorities have the potential to unnecessarily limit innovation in mobile payments products. It would be unfortunate indeed if regulations prevented true innovation in the payments system, a system deemed by many as prohibitively expensive and “broken”. Yodo’s Mobile Money system has been designed with and for altruistic goals of enhancing financial inclusion and in particular in reducing the exorbitant cost of international remittance flows which add further difficulty for Yodo to remain compliant with present or proposed regulations.

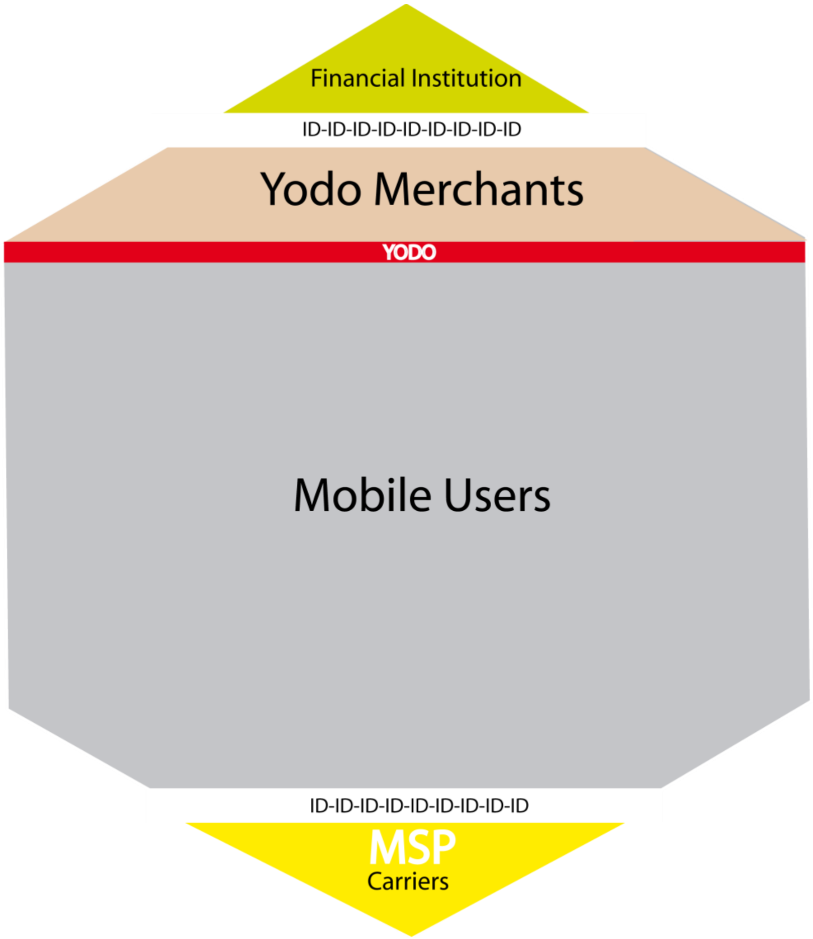
It becomes a business risk for Yodo to allow users to remain anonymous only in terms of regulatory compliance not in fraud prevention. Our product is very close to an electronic form of cash and every criteria except for compliance costs are superior not only to cash but to most other mobile money systems. Because Yodo’s mobile money (like cash) remains anonymous there are no costs to protect individual privacy and preventing identity theft one of the most frequent and lucrative forms of theft in this digital age. The easiest way to protect privacy and prevent identity theft is simply never to collect this information in the first place. Unlike a system which extends credit and must be post paid it is not necessary to collect personal information when all sums of money are pre-paid.

A significant difference between Yodo, and other anonymous products such as Bit-Coins or pre-paid cards which each of which may be acquired anonymously and be transferred or shipped in bulk, is that pre-paid funds in Yodo accounts are explicitly tied to an expensive, physical, easily identifiable and traceable source that being the mobile handset. There is no way to transfer or to load cash to a Yodo mobile money account without having the associated mobile handset in one’s possession. Unless a criminal is prepared to purchase numerous handsets, likely under contract and with the identity requirements of the carrier to attain SIM cards, it is not possible to use Yodo to create a large enough flow of cash to become a cost efficient and worthwhile exercise in illicit cash movement.

Yodo enforces strict rules on the amount of pre-paid money, or the maximum balance a user (handset) may have. Again unlike other pre-paid access product such as for example pre-paid cards which can be purchased anonymously in high volume and easily moved in bulk across international borders it is much more difficult and unlikely that organized crime would purchase bulk quantities of mobile phones load small amounts of cash, the maximum value of which is often less than the cost of the mobile phones and attempt to use Yodo as a money laundering or terrorist financing scheme. There is also presently no allowance for cash to be loaded onto Yodo accounts other than by tendering an amount in excess of goods or services being consumed in or at a registered Yodo merchant.

Finally Yodo does near real time monitoring of all transactions and can both detect and block, or disable either individual account holders or registered merchants for which suspect , high velocity or high volume, transactions occurred.

Yodo's Mobile Money product is therefore composed of or reliant upon multiple-stakeholders which can be represented by a multi-layer stack (see diagram below). The client or consumer layer is the only layer which can remain anonymous to all layers above it. That is to say individual Yodopay users may remain anonymous to both the service provider (Yodo) and to the Merchant layer with whom they transact with lying immediately above it.



Users down load a mobile App from a website or an App store and there is no requirement for them to provide their names, provide (or even have) an address, a telephone number , a photo, a Social Security number, a driver's license or any other traditional form of identification. Yodo relies upon a hardware MAC or machine authentication code from the handset, a biometric code such as a facial template or voice print (easily attainable on smart phones) plus a user generated Personal Identity

Phrase (PIP) to positively identify or authenticate mobile users. We call this tri-factor authentication of our users - ***authentication with anonymity***. In reality the security of transaction with this tri-factor authentication and the absence of personal information to protect users from identity theft, makes Yodo's security scheme superior to most common electronic payment systems such as bank payment cards and those mobile payment providers who leverage these same bank cards. This means an individual user's privacy is absolutely protected but it does NOT mean Yodo could not track and identify an individual user to assist in a criminal investigation. In fact Yodo's user agreement stipulated that the user agrees that Yodo has the right to provide all information available on the users account and account activities when a competent legal authority so requests.

Unlike a number of countries, American and Canadian law does not force personal registration of mobile handsets. However due to the fact 80% of mobile users enter into contracts with their carriers for cellular services, plus the common practice of using a credit card online to pay for air- time of consumers on pre-paid plans, the vast majority of cellular users in North America and therefore the vast majority of mobile money users are for practical purposes identifiable with strong identification credentials. That is to say by reason of the carriers (AT&T, Verizon, Bell , Rogers, etc) strong identity requirements for the procurement of SIM cards strong identity properties for mobile handsets are created at the boundary between the bottom two layers of the stack. Only a small minority of users may elect to purchase a used or unlocked handset and rely entirely upon either Wi-Fi hot spots or "convenience store" pre-paid mobile SIM cards purchased with cash to circumvent this identity requirement.

If one looks at the Merchant layer the identity requirements are again very strong in both directions as represented by the contractual agreement in place between Yodo Inc. and the registered merchant be they a company or sole proprietorship but also by their physical premises (right down to an assigned GPS coordinates) where Yodo POS devices are permitted to operate. Move the device which serves as a conduit, or regulates the introduction of cash into Yodo's Mobile money system, from it legally stipulated operational location and the device will be blocked and no longer able access Yodo's cloud based transaction switch.

Above the Merchant layer is the financial institution which is fully regulated by and fully compliant with a number of regulatory bodies including FinCon and FinTrac. The Yodo Merchant agreement requires merchants to open a designated ***Merchant Settlement account*** where settlement funds are automatically transferred. Financial institutions also have real time monitoring system similar to Yodo's monitoring systems, which can detect and block at the merchant settlement level suspicious, high volume or fraudulent activity.

Yodo management has studied the KYC requirements for MSB and deemed the negative attributes of identifying users out-weighs the positive value. Were Yodo compelled to collect the identity of each user the greatest likelihood would be for registered merchants to complete this task upon a user's first face to face encounter. Many owners of cellular phones are minors with no, or at best poor identity documents, and often no bank cards. Yodo provides a safe method for them to transact and to learn money management skills. Yodo feels the dangers of invasion of privacy and potentially even pedophile assaults may increase should young children be forced to provide personal information to merchants.

Consider for example the photo below which shows a grade-seven girl using her phone to make a purchase at a candy store. What positive effects would there be in terms of reducing money laundering and/or terrorist funding should Yodo and by extension the Merchant be asked to collect and store personal information on the client? Which parents would approve of their young daughter providing personal information such as name, telephone and address to an unknown shop attendant?

Summary:

- Highly secure easily identified digital wallet with strong initial identity factors shared between user and mobile service providers.
- Strong mobile user authentication at time of transaction using tri-factor methods including bio-metrics and high bit-level PKI to fault tolerant cloud based transaction switches.
- Near Real time transactions and monitoring of all transactions with proximity (in person face to face) cash loading or account funding.
- Total protection of individual privacy and no exposure to payee or payer bank accounts (savings)
- Fully auditable transaction trail preventing an underground economy and tax avoidance.
- Strict upper limits on Yodo account balances tied to an easily traceable physical wallet to pragmatically prevent money laundering.
- Financial Institution monitoring of all Settlement activities between merchants typically larger and less frequent than small value consumer in retail transactions.