**Description:**

Proposed system would enable secure and private transaction for online purchases either with your credit cards, debit cards or even a checking account without carrying any plastics or checkbook. This will also enable purchasing without giving out any personal information of any sort. Any time user wants to do any financial transaction he/she creates a new one using his/her **mobile** **device**. Google wallet is convenient and already solves part of the problem but you need to use Google services and abide by its terms. Google and other ecosystems are convenient but they are becoming new walled gardens. This could be another tool to avoid credit card frauds especially online transaction frauds.

**Value Proposition:**

Benefits to End Users:

* End user doesn’t need to carry or keep track of plastics or check books.
* Protect user’s personal information from proliferating across the globe.
* We strongly believe that the retailers don’t need (and store) customers personal information to complete the transaction. Retailers can't misuse user data (like sharing or selling it to others as there is nothing to misuse).
* Convenient way of fastest money transfer to their close friends or family members in urgent need. Imagine a friend is travelling in New York City and he/she is in dire need of immediate money because he/she has lost all the belongings. In this scenario a Sender creates a virtual-transaction with all the details including a secret code (similar to a debit card pin #) and gives this information (a string) to the receiver over the phone who in turn uses it at ATM machine (or special kiosks at 7Elevan or 24-hr stores) to cash in.

Benefit to the “Providers” (Banks, Credit Card companies or other financial institutions):

* No need to design, manufacture and distribute millions of credit, debit cards or checks year after year, saving paper and plastic.
* They don't need to keep track of lost/stolen cards,
* May need to worry less about loss of millions of dollars to financial fraud due to lost/stolen cards.  The rapid growth of credit card use on the internet has made database security lapses particularly costly. Whenever it happens millions of accounts have been compromised at a time. Today’s fraud detection systems are designed to prevent a very small percent of all transactions processed which still translates into billions of dollars in losses (Business Applications of Neural Networks by Bill Edisbury).

Benefit to the Retailers:

* They can be protected from the use of fraudulent credit cards. In year 2009 BestBuy Inc., lost $100 million worth of goods to a gang of hackers/thieves who used stolen credit card information to place the orders online.
* Retailer’s benefit tremendously by getting personal information of their customer which they can use for targeted advertising. To mitigate this issue, we are suggesting another piece of information which can be as anonymous as possible like an email address could be used to advertise the products to individual customer. Email addresses can also be used to send out the receipts.

**Solution:**

* Both retailer and Provider needs to sign-up with ‘**Intel Service’**. This is like a router service which receives a virtual-transaction from the participating retailer and forwards it to the correct participating provider along with retailer information in encrypted form. Rest of the transaction completes as usual.
* For end user, there will be application (mobile or web) with common interface to all "Providers". User inputs a name for a transaction (optional), assign expiration date (optional), amount, and a pin code (optional and can be different every time if needed). The input process can be automated with few rules to make it more convenient.
* Then user submits to a "Provider" of choice at the time, who in turn generates an encrypted string or a number with a bar code (can simply be scanned at the brick-and-mortar store).
* User can use this encrypted **token**/number at online merchant (for e.g. amazon), which internally could decrypt enough information to know about "Provider". This gets sent to a Provider who can authenticate, decrypt and complete the transaction marking it as "**complete**" in the system.
* These transactions will have default expiration date/time so that transaction becomes obsolete after validity period or use.
* Every provider can have their own encrypt/decrypt technology. This gives user a freedom and improves mobile banking experience.  "Providers" will certainly need to use Intel's best and fast server technology with dedicated encryption/decryption circuitry to provide faster service.

**2nd State of the competition**

**Market Opportunity:**

1. TAM: From my market research and reports I have read, I found out that the total number of mobile payment users will reach 448 million users by 2016 from 212.2 million in 2012, according to Gartner, Inc. This presents huge opportunity in the mobile payment space. The number of U.S. digital shoppers is expected to grow from 137 million in 2010 to 175 million in 2016, according to eMarketer estimates ([www.statista.com](http://www.statista.com))

The US mobile payment market is expected to reach (<http://techcrunch.com/2013/01/16/forrester-u-s-mobile-payments-market-predicted-to-reach-90b-by-2017-up-from-12-8b-in-2012/>) 90 Billion by 2017.

1. SAM: In this space PayPal has the highest market share (in terms of customer who uses PayPal solution) of around 100 million customers. Other customers are being served by Google using NFC technology along with individual solutions by each major credit card companies. This technology could be integrated with retailers/providers using NFC based solution for payment processing.
2. SOM: My strategy is to work with Major bank(s) or a Credit Card companies to license/enable this technology/idea, and develop an application interface for retailer to use this system. After going to market I'm expecting signup of at least 1% of 100 million of PayPal's customer or new customers from uBid.com or similar auction sites, of around 1 million customers to start using this system in the first year. In this case I'm assuming 10 million transactions a month with 0.5% charge per transaction would generate approx. $500,000 by first year. This is very realistic and reachable target by end of first year of deployment. With growth rate (new customers and transactions) of 10% in next 2 years, my revenue will be $1.2M by year 3. Additional revenue will be generated by anonymous data analysis services to the retail sector.

**Competitive landscape**

Mobile payments market is growing very fast with many new startups and also products from incumbents like Paypal, and Intuit. PayPal’s “Here” is a service is similar to SquareUp with better features. There are other companies like Braintree that are providing encrypted tokens to make payments. There is significant traction for PayPal services in the market due to brand recognition. “SquareUp”, “SumUp”, “iZettle”, “Payleven” and other companies are providing mainly card readers (dongle based) for the individual sellers or small businesses to carry out mobile payments with customers. They charge 2-3 % of the transaction as a fee. **PayPal’s “Here”** is an App based but still charges the same fee. We are charging a small fee for letting our customers use the service and they also get the benefit of anonymous transaction.

Amazon is also working on a patent for anonymous transaction.

Our sustainable advantage is being able to protect all the entities i.e. banks, consumers from fraud due to loss of credit cards or credit card info while providing banks with more revenue thru small businesses who can use our service with much lesser overhead. We have the added benefit of collecting data (though anonymous) that is location based that has invaluable to marketers. Encrypted card readers can be easily hacked since they are used repeatedly with same encryption. Our encryption system can use different encryption technologies and can be dynamically changed by providers making it difficult to hack into the private data.

**Go To Market Model and Value Chain**

We will partner with credit card processing getaways and banks to enable processing credit card, debit card and check transactions. We will target online retailers and small businesses in local geography as our first customers. We will market to them directly and through small business associations.

**Business Model**

Our customers are small business owner or individual who currently uses service like PayPal. The customers will pay us a percentage of their revenue of the transactions. We will charge a fee to the merchants. For all successful transactions this will be deducted before money is transferred to their account thru the bank card processing gateways.

For a $100 transaction the business owner will get $99.50 minus the bank credit card fees if any. We will provide customer service through email and phone or online chat support.

**Market Acceptance**

PayPal’s “Here” service and Braintree’s “token” based payment service are some examples where this idea has been accepted by consumers and merchants.

Paritosh,

Thanks for your comment and interest. Yes the whole premise is that, merchants really do not need really any personal information to do business. In fact PayPal's service is being accepted at Home Depot now, which behaves exactly the same way. Also this could be a differentiation factor for various small businesses to attract customers. In small business case, we can provider 'Data Analysis' service which will be based on anonymous data gathered across similar business across town, city, state or nationwide which effectively could compensate this risk,

Since this service will be rolled out to the online businesses first, "Card present" will be moot at least initially. Also as you said, this is done to make someone liable for fraudulent transactions. My thinking is this service will be good option against the fraud. But it would be really useful to get some real feedback by talking to some targeted customers like various auction sites where anonymity is utmost importance.

.