Securing the Uncharted Territory: Transaction Receipts in Branchless Banking

Saurabh Panjwani
Bell Labs India,
Bangalore, India
saurabh.panjwani@alcatel-lucent.com

Mohona Ghosh, Ponnurangam K,
Soumya Vardhan Singh
IIIT Delhi,
Delhi, India
{mohona1011, pk, soumya10086}@iiitd.ac.in

ABSTRACT

Mobile-based branchless banking has become a key mechanism for enabling financial inclusion in the developing regions of the world. A fundamental requirement of all branchless banking systems is a mechanism to provide reliable evidence to users about the occurrence of transactions, which is implemented in the form of receipts delivered after each transaction. Existing receipt delivery mechanisms, however, provide poor security guarantees to users, which has led to multiple exploits and financial losses recently. In this paper, we present results from two studies conducted with users of a leading branchless banking service in India. Our first study explores current practice with respect to transaction receipts through interviews conducted with 67 users and 87 transaction observations. The study reveals a desire for robust receipt delivery systems amongst users as well as a prevalence of insecure practices, which makes users susceptible to fraud. The second study tests usability of receipt verification protocols with 30 users and finds that despite their limited education, users are able to distinguish between secure and insecure interfaces for receipt verification and 37% of them state a strong preference for the secure interface even though it is evidently less convenient.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: Miscellaneous; K.6.5 [**Security and Protection**]: Miscellaneous

General Terms

Experimentation, Human Factors, Measurement, Security

Keywords

Branchless banking, mobile, receipts, security, user study

1. INTRODUCTION

Branchless banking systems are becoming prevalent in the developing regions of the world as a mechanism to extend financial services to the economically deprived populations. Instead of setting up formal bank branches and ATM outlets, these systems use a network of human agents to facilitate banking transactions, thereby reducing the cost of banking for people with small cash holdings. Today, over 50 million people in the developing world rely on branchless banking services to meet their financial needs and together they transact more than $100 million on a daily basis [12].

Mobile phones play a central role in branchless banking, owing to their low cost and deep penetration in the developing world. Transactions typically involve a bank customer and an agent meeting in one location, exchanging messages with a remote server (operated by the bank) using their mobile phones and giving cash to, or taking cash from, the other party. At the end of each transaction, parties normally receive a confirmation or a "receipt" from the bank server which serves as evidence of transaction completion and can be used in situations of disputes later on. In many systems, receipts are sent by the bank server in the form of an SMS to the transacting parties' mobile phones and these SMS'es contain critical information like the amount transacted and the affected account number.

While mobile technology has yielded efficient mechanisms for facilitating finance in the developing world, it has also given rise to novel security challenges. SMS'es can be spoofed, quite easily nowadays [3], and the GSM standard, which is the widest utilized telephony standard in the world, provides limited native support to enable phone users to verify the source and authenticity of messages they receive [15]. Current branchless banking systems provide no additional support for authenticating receipts and in fact, at least two of them have already been subjected to spoofing attacks that have caused significant financial losses to both users and providers. (See Section 3 for more.)

In this paper, we present findings from two studies conducted in collaboration with a leading branchless banking service provider in India. In our first study, we investigated current practice with respect to the use of SMS-based transaction receipts by interviewing 67 bank customers and agents and observing 87 real transactions. We find that although customers desire reliable transaction receipts from the system and view them as essential proofs of transaction occurrence, their understanding of the current receipt delivery technology is rather naive and they tend to make weak claims about its security. Furthermore, customers are easily persuaded by banking agents into deviating from prescribed rules, which increases their susceptibility to fraud and malpractice. In the second study, we evaluated the us-

ability of a receipt verification protocol involving the use of one-time passwords across a sample of 30 users of the same service. We find that 37% of the users state a preference for using the protocol (over an insecure baseline), due to self-perceived security benefits, even though it requires significantly greater effort and attention. This finding contrasts with results from other studies in the literature on usable security in web banking transactions, where secure protocols were found to be less preferred due to usability barriers.

2. BACKGROUND AND RELATED WORK

Using mobiles for commerce is becoming widespread in the world, both in developed and developing societies. Our focus in this work is on a specific type of mobile banking, called *branchless banking*, which is unique to developing regions. A critical component of these systems is the presence of a human agent who interfaces between customers and the service provider and facilitates cash-based transactions, much the same way as ATM machines and bank tellers enable them for regular bank users.

Transactions work as follows: A customer visits an authorized banking agent, who typically operates a small mom-and-pop shop in a market area (his primary source of income), and makes a request for a cash deposit or withdrawal. Either the agent or the customer sends a message with relevant details, like the amount of money to be transferred and the target recipient details, to a remote server using his mobile phone. The message is usually sent using a basic messaging protocol like SMS that is available on all phones, and is accompanied with suitable credentials like a secret PIN or other identification information unique to the message sender. The server looks up a central database and either approves the transaction or denies it and subsequently sends a notification to both the agent and the customer, again via a basic messaging protocol like SMS. If both parties receive a positive confirmation on their phones, they exchange the desired amount of cash; the agent receives cash from the customer in the case of deposits while the customer receives cash in the case of withdrawals. Some systems also implement a money transfer facility wherein the customer either submits real cash to the agent and the agent sends the transaction request message to the bank, or the customer herself sends a request to the bank for an electronic transfer; transaction receipts from the bank are critical here as well.

The cost of providing banking services through agents in this manner is often lower than that of setting up brick-and-mortar offices in developing regions, which is why branchless banking is finding significant penetration in these regions. In India, 60% of the citizens are still without a bank account[1] and even amongst those who have an account, a large fraction is "under"-banked in that access to a banking facility is a challenge for them, either due to geography or due to congestion in bank branches. To benefit such people, at least seven branchless banking services have been launched in different parts of the country only in the last 4 years and today, these systems are touching more than 20 million users already.

2.1 Risks in Branchless Banking

With the reduced costs and convenience of operating financial services through agents and phones, comes new opportunity for abuse. Much of the risk in running branchless banking systems arises from the infrastructural limitations under which they operate. In order to make the service accessible to people in the developing world, service providers generally design their communication protocols so as to be operable on basic phones which support only calling and texting. Some systems do assume agents to have phones with advanced capabilities (e.g., data connectivity), but even with this assumption, the vulnerability of customers remains high.

While one could list several potential threats to branchless banking systems (see [16] for a discussion), there are two which seem most relevant to practice. The first is an attack in which a malicious user or an agent tries to operate an account (e.g., withdraw money from it) that he/she is not authorized to operate, e.g., by stealing the victim's phone. All known branchless banks implement a defense against this attack by requiring that users—both agents and customers—submit suitable credentials along with any transaction request. User credentials are protected from theft using a variety of techniques, sometimes by programming the SIM card of the user's phones [2], sometimes by using special security tokens [1], sometimes by relying on the peculiarities of voice biometrics[2], and sometimes not at all[3]. Panjwani and Cutrell provide a detailed discussion on this topic [17].

The second serious threat to branchless banking is the forgery of receipts that are sent by the bank to users after every transaction. False receipts can cause users (both agents and customers) to yield cash even when a transaction has not taken place. All existing systems use either SMS or plain paper for communicating receipts to users and spoofing such messages is easy, given recent technological advances [3]. None of these systems equip users with a method to verify authenticity of receipts and in multiple events in the recent past, miscreants have exploited this weakness and caused significant financial damage to service providers (Section 3). It is this threat which forms the focus of our work.

2.2 Related work

Despite the rife deployment of branchless banking, research on security and usability issues in these systems is in a fairly nascent state. Recent work from the systems community discusses the challenges associated with security design for branchless banking [15, 16], but unlike the domain of ATM-based banking and credit card commerce, no systematic standards of security have yet evolved. Providers generally tend to rely on ad-hoc security practices, which are typically not made available for public scrutiny and analysis.

The difficulty of designing secure banking protocols for developing world phones raises novel usability challenges, too, which form an important thread in our paper. Closely related to our work is the work of Medhi *et al.* [13], where the authors used a rich ethnographic study across four developing countries to show that text-based interfaces are difficult to navigate for most candidate branchless banking users. Their work, however, has limited discussion on security issues in branchless banking or on user perceptions of security. Furthermore, [13] makes recommendations for user interface

[1]Reserve Bank of India. Harnessing Technology to Bank the Unbanked. http://rbi.org.in/SCRIPTs/BS_SpeechesView.aspx?Id=509

[2]BASIX Sub-K (http://subk.co.in/)

[3]G-Cash (http://site.globe.com.ph/web/gcash)

design of branchless banking systems *in general* while we focus on improving the system interface to address one *specific* security issue—the forgery of transaction receipts—which has become quite relevant after recent events of fraud.

Kumar *et al.* [11] present an ethnographic study on payment practices in India and based on their study's findings, provide design guidelines for future mobile payment and banking systems. They emphasize how paper receipts are central to several cash-based transactions in India and sometimes, play roles other than that of a transaction proof as well. While the study brings out the potential value digital receipts can bring to monetary exchanges in developing countries, they do not discuss security issues in receipt systems, which is where our contribution lies.

Our work contributes to the recent line of research on understanding and designing for security problems that are unique to the developing world [5, 6, 17]. We believe there is rich opportunity for doing work at the intersection of usability and security in solving these problems, as technology spreads rapidly into developing regions, applications become varied and security-sensitive, while growth in education and literacy of the population remains gradual.

3. ABUSE AND FRAUD IN REAL SYSTEMS

In February 2010, M-Pesa [2], the first branchless banking service in the world with a customer base of over 10 million users across 4 countries, was subjected to an attack involving the use of spoofed SMS'es[4]. A malicious customer approached an agent working in a peri-urban locale in Kenya, with a request to withdraw a large sum of money from his account. As is customary in M-Pesa withdrawals, the customer initiated the transaction by sending a message through his mobile phone although in this case, the message was sent to an accomplice on the network instead of the real M-Pesa server, which is the target recipient for genuine transactions. The accomplice instantaneously forged an SMS receipt for the transaction, tagged it with a genuine-looking sender ID and sent it to the agent's phone, claiming a record of the transaction on the actual server. The agent, not being able to tell the SMS apart from genuine receipt messages, was persuaded into yielding the cash to the customer. About $450 worth of money was lost (more than ten times the average M-Pesa transaction value[5]), and it appears that the agent was never compensated for this loss by M-Pesa [8]. There are reports that multiple instances of this attack have been launched against M-Pesa agents [8]. No fixes to the system are publicly known yet.

In another case of fraud in India, a branchless banking service provider named Eko [1]—also the subject of our research—suffered financial losses at the hands of malicious *agents* misimplementing money transfer transactions. Customers would approach an agent, hand over cash to be deposited into a remote relative's account, and the agent would provide a hand-written paper receipt for the transaction, claiming that the SMS receipt from the server would arrive on the customer's phone later when the "server is available". No messages were ever sent on the network and a large sum of money was lost to multiple such agents [Eko, personal communication]. Although in these cases, the attackers apparently did not use SMS spoofers to defraud customers, the incidents did reveal the possibility of malicious intent on the part of the agents and the importance of building tools to enable customers to verify fulfillment of transactions (and to train them to use the tools effectively). A senior technology officer at Eko shared his thoughts on SMS spoofing, *"While it is easy to spoof an SMS, certain elements could be added to the transaction receipts that would make such a spoof easy to spot. We are working towards strengthening our system to protect it against spoofing attacks."*

[4]Telco 2.0. *Security Breach at M-Pesa.* http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html

[5]Paying the piper: http://comm.ae/2009/02/17/paying-the-piper/

4. A STUDY OF CURRENT PRACTICE

We began our research by investigating current practices and user perceptions with respect to transaction receipts in the context of Eko India Financial Services, one of the most actively-used branchless banking services in India. Eko is a business correspondent of State Bank of India (SBI), the leading public sector bank in the country and through its network of more than 1300 agents, serves over a million customers in the peri-urban areas of Delhi and mid-sized towns in the states of Bihar and Jharkhand.

4.1 The Eko System and Interface

Eko's primary service offering is money transfer, which is intended to work as follows: A customer approaches an Eko agent with the money to be transferred (in cash) and the agent sends a USSD message[6] to an Eko-operated server with relevant details like the amount to be deposited, the target account number and some information necessary to authenticate the agent to Eko. Once the transaction is recorded at the server, both the agent and the customer receive an SMS confirming transaction completion. Upon seeing the confirmation, the customer submits the cash to the agent, along with a fee of roughly 1%, out of which 0.25% is later channeled to the agent as commission. The service is mainly targeted at low-income migrant workers in urban India who regularly need to send money to distant relatives but due to residency and other requirements, are unable to acquire a personal bank account to accomplish this. There are indications that over 2 million people of this type live in Delhi alone, and more in other urban areas[7]. Such people, who would earlier either rely on expensive methods like the post office and human couriers, or spend numerous hours standing in queues at SBI bank branches, can now use branchless banking services like Eko to meet their needs. Eko reports a daily transaction volume of more than Rs.50 million ($1 million)[8] in its money transfer offering.

For a successful transaction, the SMS receipt sent to the customer has the following structure (see figure 1 (a)): it begins with the phrase "Deposit Successful" after which it shows the amount transferred and then the SBI account number of the depositee. Following these, the receipts contain several secondary fields like the fees deducted for the

[6]USSD stands for Unstructured Supplementary Service Data, a protocol that is usually more reliable and efficient than SMS, but uses a more restricted message format.

[7]Census of India 2011 Migration Report. http://censusindia.gov.in/Ad_Campaign/drop_in_articles/08-Migration.pdf

[8]We use an exchange ratio of 1 US dollar (denoted $) to 50 Indian "rupees" (denoted Rs.) throughout the paper.

transaction, the phone number of the agent, transaction time and a transaction ID, written TID. Users of basic phones often need to scroll down the SMS to view these fields. (In the agent's receipt, instead of the first two of these fields, the current float value of the agent and the commission earned are depicted.) The TID is the same for both receipts and indexes the transaction in digital records. The sender ID in both receipts is "TD-SBI-Eko". All fields are named in English, which is not the first language for users (Hindi, in most cases) but easier to implement on SMS.

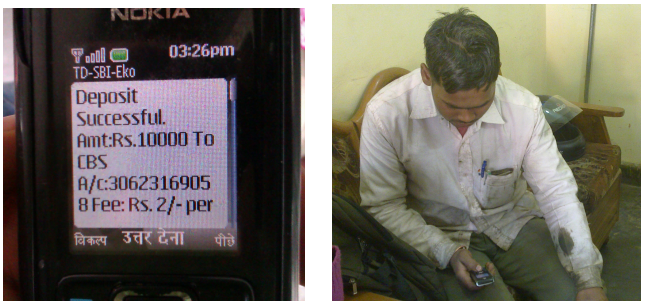
Eko provides phone-based customer care service to customers and agents. Users can call this service and a pre-recorded voice speaks out, in Hindi, the details of the most recent transaction done using the calling phone. If further information is needed, the call is routed to a call center.

Besides money transfer, Eko also offers the facility to open "mini" savings accounts with SBI for people who cannot afford regular bank accounts. Such accounts are easier to open (fewer enrolment criteria) but can be operated only at Eko service outlets. The Reserve Bank of India (RBI) regulates volumes in such accounts and Eko enforces suitable upper limits on transaction values. Customers can deposit money into these accounts (using a protocol similar to the money transfer protocol), check their balance, withdraw money and transfer money into other mini savings accounts directly using their phones. (For the last two types of transactions, suitable customer credentials are required to be sent to the bank.) Receipts are similar to money transfer receipts. Although this service of Eko pre-dates the money transfer service, its current utilization is significantly lower ($10,000 daily transaction volume); as such, we focus our discussions on Eko around money transfer transactions.

4.2 Method

We spent several hours visiting Eko's service outlets in peri-urban areas of Delhi, talking to agents and their customers, and observing customers carry out transactions. Our conversations were one-on-one, semi-structured interviews and centered around users' understanding of and perception towards transaction receipts. We reached out to users through a two-step process. We first sampled 15 agents from a long list provided to us by Eko, ensuring a broad geographic spread in the city (8 locales of Delhi were covered, each at least 5 km or 3.1 miles apart from the other). We visited these agents, most of whom operated a mobile service shop in the heart of a slum and interviewed them consensually, while they conducted their daily affair. In parallel, we waited for Eko customers to visit. Where feasible, we observed customers conduct transactions and post the transactions, based upon customer consent, took them away for an interview. A few customers were approached for interviews via phone calls. We spoke to 52 customers (which included 7 mini savings account holders); summed with the agents, this gave us a sample of 67 users. We observed 87 transactions, out of which all but 3 were money transfers. Interviews were conducted in Hindi, the common language across all users, and responses recorded on paper. All users (customers and agents) were suitably compensated for their time. Put together, the study involved spending over 140 man-hours in the field.

Ethics. Since our study involved discussions and observations around banking transactions, which are generally



(a) (b)

Figure 1: (a) An SMS receipt for a successful money transfer. (b) A customer views an SMS receipt while sitting in an agent shop. Receipts arrived immediately after transaction completion in most cases, though some customers claimed to wait for 2 days for them.

treated with privacy by users, we maintained some ethical guidelines constantly during our study. We followed a standard informed consent protocol for all our interviews and did not query subjects about sensitive details like their account balances which were not relevant to the study. Our observations were made from a distance which enabled us to view user behavior without leaking private credentials. Most of the observed transactions were money transfers, which require no credential input from the customer (only the agent submits credentials); as such, standing on the opposite side of shop counters enabled us to make observations in a privacy-preserving manner. Photographs were taken with consent of the relevant parties. While our observations did leak some information about transactions non-consensually (e.g., we learnt information like "account X was credited with amount Y at time T"), we did not record all such information in writing (e.g., account numbers were not recorded); even what was recorded, will be deleted at the end of the research.

User profiles. Our interviewees had limited education, twenty (i.e., about 30%) not having made it past 8^{th} grade and a majority (75%) not having made it to college. Agents were consistently better-educated than their customers, although we found one agent who studied only till 6^{th} grade and was without a less-educated customer. Our estimate is that less than half of the users have monthly incomes greater than Rs.10,000 ($200) though we could not verify this in all cases. There was only one female agent in our sample, which is reasonable given that less than 5% of Eko agents are females. Even amongst the customers, we met only three females (6%) who consented for an interview, not very surprising given less than 10% of Eko's customers in Delhi are females. A majority of the customers we spoke to were migrant workers engaged in occupations like that of manual labor, driving, cooking, supervising contract labour and operating a small business and used the money transfer facility of Eko for remittances. A few of them were local residents who used the facility to pay salaries to employees in their businesses; while the employees themselves resided in Delhi (without a personal bank account), their salaries would be transmitted to accounts of remote family members in their respective home-towns.

4.3 Findings

Money transfers observed by us ranged from Rs.1000 ($20) to Rs.10,000 ($200, the daily limit) although the bulk of them (about 40%) were in the range $40-$100. Customers often used Eko to move almost their entire monthly income to their remote families in a single transaction, leaving only the bare minimum for local consumption. Agents reported to be transacting at least $1000 daily, but we heard one report of a day's transactions exceeding $10,000, a sizeable sum given that agents' daily income from Eko rarely exceeded $10. Most of the agents paid a daily visit to a nearby SBI branch to transfer the collected cash to the bank and update their floats, though the busier agents distributed the risk of carrying cash across multiple visits (three daily visits in one case).

We now report our key observations regarding customers' and agents' usage of transaction receipts in the Eko system.

4.3.1 SMS Woes

While both customers and agents expressed a high degree of satisfaction with Eko's services, we heard numerous concerns about intermittent system outages and the unreliable nature of the SMS receipts. Delay in SMS delivery was a grievance reported by nearly all the users we interviewed. Some customers reported delays of up to 2 days in receiving their SMS receipts although in our own observations, we saw that for the majority of the transactions (more than 70%) an SMS receipt did arrive on the customer's phone within 2 minutes of transaction initiation (agent sending the USSD message). We observed only 14 transactions (about 16%) in which the customer did not receive an SMS receipt for 5 minutes or more. In about a third of these cases ($n = 5$), the customer explicitly asked the agent for a resolution or waited patiently at the shop till SMS arrival (more than 15 minutes in one case); in the rest, the customer left the shop without complaining.

Very few customers seemed to call Eko's customer care in situations of SMS failure or delays, even though information about customer care was conspicuously displayed in every shop we visited. We observed only 4 cases of calls being made to customer care; in all cases, it was not the customer but the agent who was attempting to resolve the situation on behalf of the customer. Even in our interviews, few customers (less than 20%) reported to have called customer care themselves in the past; in fact, 25 customers (nearly 50%) were not aware of the service.

An important source of confidence in the system for the customers was the acknowledgement they received from the target recipients. When asked about possible solutions to the SMS delay problem, one customer retorted: *"What is the need to solve this problem? The person I send the money to himself tells me whether he has received it or not."* We noted two customers who called their target recipients right from the shop's premises where they transacted and informed them about the transaction. One customer claimed during his interview that his recipient would often station himself at the respective bank branch when a transaction was being carried out and, within minutes, call back to confirm receipt of the money.[9] However, the average acknowledgement delay was reported to be greater than 1 day (the maximum being 7 days), and explained by the difficult access of bank branches and ATMs for target recipients. This makes recipient acknowledgements of limited appeal as a standalone security measure.

4.3.2 Introduction of Paper

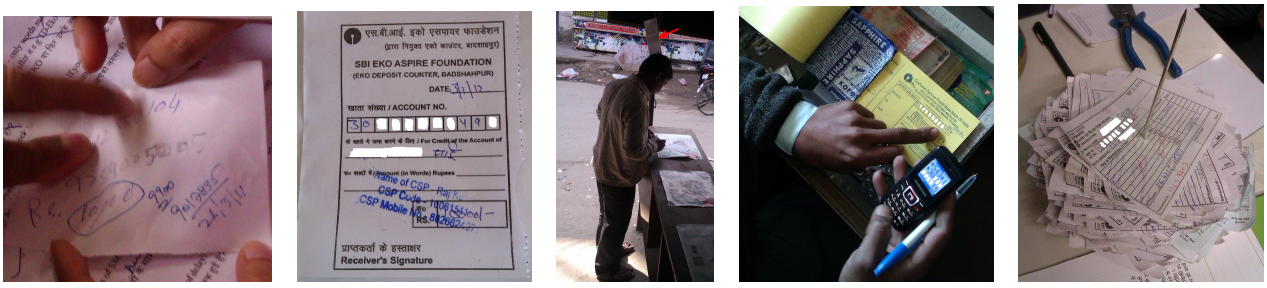
In order to cope with the unreliability of SMS, several agents had proactively implemented an alternate form of receipt delivery mechanism in their shops. Out of the 15 agents we spoke to, 11 had initiated a practice of giving out *paper* receipts to customers as a way to supplement SMS. A common explanation given to customers was: *"Even if the SMS is late, this is proof that [you] made the deposit."* Paper receipts were also a strategy for convenience: some agents would collect cash from customers, hand over a paper receipt but delay the implementation of the transaction for later when it was more convenient for them to implement it. This not only increased operational efficiency (agents could batch process multiple transactions in their free time) but also improved availability (they could accept transaction requests from customers during server downtime). Up to 9% of an agent's income from Eko was supposedly spent on buying paper for these receipts alone.

Agents seemed to be constantly experimenting with different techniques and formats of paper receipts in order to maximize customer confidence and minimize service time. In most of the shops, the practice was reported to have started by writing down transaction details (particularly, the amount, account number and TID) on a piece of scratch paper and giving it to the customer to use in case of future disputes about the transaction (figure 2(a)). Some agents continued with this practice at the time of our visits, but more than half had transitioned to a system of structured, pre-printed sheaves of paper which would be filled out as transaction requests came in. The sheaves were designed to mimic receipt booklets commonly seen in bank branches in India[10] and often had details in addition to those in Eko's SMS receipts (although they didn't necessarily contain all SMS receipt details). For example, the names of the intended recipient and of the agent and a signature from the agent were common additions and the TID a common omission (figure 2(b)). A logo of SBI was always present near the top of each receipt along with a mention of the agent's association with Eko. Furthermore, some agents had started using custom-made rubber stamps to stamp each receipt; the stamps contained agent identification information (e.g., agent name and an agent "code" provided by Eko) and, sometimes, the date of transaction as well. The text used both English and Hindi (the hand-written text tended to use Hindi only) and there was provision for the agent to retain a copy of each receipt, with space for the customer's signature.

A step further in the evolution of the paper receipt phenomenon was sourcing the receipt-filling activity to the customers, which we observed in four of the shops we visited. To avoid crowding near the counter, one of these agents (owner of an electric equipment shop) had created space outside his shop—partly encroaching on a nearby street—with an as-

[9]Indeed, the efficiency of money transfers was the most attractive feature of Eko which, seemingly, made customers prefer it over multiple other remittance services, including the services at SBI bank branches in Delhi themselves which, though cheaper than Eko, would take a day to complete transactions end-to-end.

[10]In fact, in one location we noted the use of actual bank receipt booklets which had been surreptitiously acquired from a nearby SBI bank branch.



(a) **(b)** **(c)** **(d)** **(e)**

Figure 2: Several agents had started using paper receipts as a way to supplement SMS. (a) An informal receipt written on scratch paper. The amount is circled and the TID and date written below. The account number is occluded by fingers. (b) A more structured receipt containing fields like recipient name (filled by the agent) and depositor's signature (unfilled). A stamp containing details of the agent is imprinted. (CSP stands for *customer service point.*) Details are erased for privacy. (c) A customer fills out a receipt with transaction details before making a transaction request. A sheaf of blank receipts hangs off a pole (red arrow). (d) Agents used filled receipts for entering transaction data into their phones and creating the desired electronic message. (e) A copy of all transaction receipts was maintained by some agents in piles like these.

bestos shed and a makeshift table against which customers would stand and fill out blank receipts (with key details like account number, amount and recipient name) before entering the shop. (See figure 2(c).) The counter itself had been partially glass-walled to give the appearance of an official bank counter. (Electrical equipment was sold over the unwalled area.) Delegating receipt filling to customers not only saved the agents the trouble of preparing each receipt from scratch (receipts only needed to be stamped/signed by the agent), but also eased the process of data entry into phones while creating electronic messages (figure 2(d)).

The use of paper receipts, as done by Eko agents, reduces traceability of transactions, and opens up an obvious opportunity for abuse. Eko disallows the use of these receipts as a tool to *delay* transaction execution and emphasizes the importance of viewing the SMS (and calling customer care in case of SMS delays) on its posters and banners at the agent shops. Still, such practice persists in several sites (all but two that we visited), and reflects the tight relationship of trust that customers and agents normally share with each other. Unfortunately, it is this trust which has also been violated in recent events.

4.3.3 Receipt Viewing

A majority of the users in our sample (93% agents, 65% customers) reported to be reading Eko's SMS receipts on a regular basis, although apparently with varying degrees of attention. When asked to recall contents of the receipts, sometimes right after a transaction, the only field that users could consistently recall was the "amount". Twenty customers (38%) in our sample could not recall the existence of the *account number* in the SMS receipts (although all either spoke or wrote it out before transactions) and several more did not remember the existence of the TID. At least 16 customers (31%) could not even *recognize* the TID, even when told about it.

Evidence from our observations was not perfectly aligned with customer reports: Out of the 87 transactions we viewed, the customer did not make eye contact with his/her phone during the transaction in 47 (i.e. 54%) of the transactions; in 7 of these cases, the customer did not even *bring* the phone to the shop for the transaction. Several of these customers seemed to be sensing the arrival of an SMS (via a phone alert) but most did not give an indication of wanting to view SMS receipts at the shop.[11]

It was clear that the issuance of paper receipts was influencing this behavior—at shops where paper receipts were not issued, nearly all customers made a visible effort to read the SMS receipt (and to complain against delays). On the other hand, customers who had been exposed to paper receipts made statements like: *"Paper receipt is excellent! The SMS may or may not come but the paper serves as proof."* The paper receipt became a persuasive tool for the agent to pacify customers distressed by SMS delays: we witnessed 3 cases in which the agent initiated a transaction, the customer's SMS was delayed, the customer complained and the agent consoled him/her, saying that *"paper serves the same purpose as SMS".*

Familiarity with the system seemed to further effect the degree to which SMS'es were viewed: the newer customers were more likely to view them than those who had used the system multiple times. Although we did not verbally verify "newness" of the customers during transactions, it was easy to spot first-time users using visible cues; every first-time user we spotted waited at the shop till his SMS receipt arrived. One of the old-timers said in his interview, *"Earlier, I used to check all details but then, when I started trusting the agent, I stopped checking. Now, I don't worry if the SMS comes or not."*

Literacy and comfort with technology seemed to have some effects, too. We met 3 customers who were completely illiterate in English and attributed their ignorance towards SMS receipts to the latter's unintelligibility; they rated the paper receipts to be more readable. Some of the literates preferred paper for readability reasons, too: *"In SMS, I have to scroll to view details; on paper, I can read everything in one go."* The female agent in our sample defended her paper receipt practice entirely on the grounds of limited literacy of her customers: *"This is India, not America. [Here,] paper re-*

[11] Conceivably, some of them viewed it after leaving the shop's premises, something we did not observe in our study.

ceipts act as token of faith that a transaction has happened. Many of my customers are laymen in terms of SMS usage."

Despite the increasing reliance on paper receipts across locations and the evident apathy towards SMS receipts during transactions, we found that the majority of the customers continued to see value in SMS and treated SMS receipts as a key indicator of transaction fulfillment. A regular user of both SMS and paper put it most succinctly, *"I have more trust in SMS [than paper]. Even if I get a paper receipt, it does not mean that the money has reached."* We saw the same view echoed by multiple users in our sample, including some of the low-literate ones. One customer cited the absence of SMS receipts in other remittance services in nearby areas as a reason for his siding with Eko. At least 22 out of 36 (i.e. 61%) customers who transacted paper receipts stated an overall preference for SMS; 12 of these 36 (i.e. 33%) wanted SMS because they felt it provided them greater confidence than paper.

4.3.4 Receipt Storage

Users (both agents and customers) tended to preserve receipts after transactions, at least till the time they remained in our sight. We did not witness any transaction in which the customer deleted the SMS or discarded the paper receipt (where issued) within the shop's premises. However, nearly half of the customers whom we interviewed reported that once they got confirmation from the target recipient regarding receipt of the money, they would delete their SMS (or if a paper receipt was issued, throw it away). From our conversations, it was apparent that customers viewed receipts as a key instrument to contest potential misimplementation and malpractice and that trusting oral promises of the agent was, in general, not enough.

There were, of course, the more cautious ones, who liked to store receipts for much longer than the norm. At least 4 customers reported that they never trashed their paper receipts and 2 claimed that they had stored all SMS receipts for Eko transactions in their inboxes. An interesting, and counter-intuitive, perception we observed across customers was that paper had a longer life than SMS. Customers felt constrained by the limited capacity of their phone inboxes: *"My phone can store only 20 messages. I delete old [receipts] when it is full."* At least 11 customers (21%) claimed to be deleting SMS receipts only because of space limitations. One agent claimed that he had stored copies of paper receipts for each transaction conducted by him in the past 9 months in an iron trunk, in case someone from the bank makes an inquiry on his huge transaction volumes. He preferred this practice to maintaining the logbook provided by Eko since his receipts carried more data items than the columns in the logbook. He ridiculed the idea of using SMS to store transaction history.

At the other extreme were customers who swore by SMS because they felt it was more convenient to maintain. Example quotes: *"The paper receipt gets lost. How do I take care of it?"; "I don't need to store SMS separately. It's always in my pocket."* Indeed, customers who preferred SMS over paper, stated convenience as their main reason (besides the trust factor) for this choice.

A few customers voiced privacy concerns with respect to their receipts (both SMS and paper). Although the majority seemed comfortable showing us the contents of their receipts individually (when we took suitable consent), our requests for *photographing* the receipts were met with noticeable resistance. *"Why do you want to photograph it?", "Is it necessary?", "You can take a picture but first, let me hide the account number with my hand."* (We took photographs only in situations where it was obvious that the customer was comfortable with our action.) The believers of receipt preservation seemed to be exercising special care in storing paper receipts at home (e.g., storing it in one place and, in one report, keeping it in a dedicated box). Though privacy concerns for receipts were not universal, it was clear that at least some customers maintained constraints on how to share information about deposit activities in their or their family's bank accounts.

4.3.5 Discussions Around Receipt Spoofing

By and large, users displayed a high level of confidence in Eko's SMS receipt technology and were not aware of the possibility of SMS'es being spoofed. When asked how they verified that the SMS'es originated at Eko and not elsewhere, at least twenty-six customers (50%) reported to rely on the sender ID they contained. Nine (17%) reported to rely on the correct presence of the "amount" field in the message. Eight customers said that they knew the sender was Eko because *"it comes immediately after the agent sends the message."* Interestingly, two customers thought that it was not Eko, but the *agent*, who was sending them the SMS receipts.

News about fraudulent transactions in other branchless banking outlets did not seem to have reached any of the customers we spoke to: none reported it proactively and amongst the fifteen that we polled (arguably with some difficulty), awareness was absent. Most customers admitted never to have thought about the possibility of receipt spoofing. In the words of one regular customer, *"Only God knows whether it is Eko or someone else who is sending the SMS. I just have faith in this (points to the phone). I never felt suspicion."* A few argued that spoofing is impossible because of factors like the immediacy with which the SMS arrives and its contents: *"How could it come from the wrong place when the amount is correct and it comes so quickly?"*, questioned one of our interviewees. One of the agents added a different perspective: *"Who has the ability to forge an SMS? Who has the vested interest? It is just not possible."* Clearly, some of these beliefs are misplaced as evidence from real-world incidents suggests.

Some users, whose suspicions were raised by our inquiry, expressed curiosity for solutions to the spoofing problem; to quote a customer *"I never thought about this, but do you have a method using which I can find out if it is Eko who sends the SMS or not?"* Another spoke: *"You are more educated than I am. You should tell me how to do this."*

While the majority of the interviewees voiced faith in the current SMS delivery system of Eko (till our inquiry began), there were six users in our sample (2 customers, 4 agents) who expressed serious concerns about spoofing. *"SBI-Eko anyone can write in an SMS, it is not difficult these days. The system runs entirely on faith,"* said one agent. When asked about how the system could be improved, users offered interesting suggestions involving terms like "secret code", "lock and key" and "a stamp from the bank". In the words of one of the customers:

"If the bank could use a secret number to send us the SMS, we could check that the SMS is from the bank. Tomorrow, the [agent] could go away but we should still be able to go to

the bank and show that we have the right SMS. "

4.3.6 Summary

In summary, the findings from our first study suggest that:

(a) Customers generally view transactions receipts (either in the form of SMS or paper) as an important component of Eko's branchless banking system: a majority of them view receipts after every transaction, maintain them securely (at least for some duration) and treat them as evidence of transaction occurrence;

(b) Views on the right medium of receipt delivery (SMS vs. paper) are divergent and depends upon how individual customers trade off security for reliability and on their literacy levels. Most customers view paper as a valuable supplement to SMS, but not good enough as a standalone mechanism for receipt delivery;

(c) Customers have a high degree of faith in Eko's agents and are persuaded by them into practices which deviate from prescribed rules;

(d) Habituation influences behavior and customers tend to become less vigilant with receipts as they transact more with the system;

(e) Most users of the system have a rather naive understanding of the underlying technology, although there are a few who can see through its weaknesses and articulate meaningful suggestions for improvement.

Some of these observations simply call for persistent customer education and training. For example, making customers aware of the risks associated with hand-written receipts and inculcating a habit of calling customer care for transaction verification in case of SMS failures, can go a long way in protecting them (and Eko) from fraud. Eko reports to be increasing its customer education efforts across locations. However, customer education alone cannot make the current system sufficiently secure for practice. The threat of receipt spoofing, both in paper and SMS, remains, as noted by some of our users and as also confirmed by real attacks.

5. A USABILITY STUDY

A key learning from our first study was that although customers place immense trust in branchless banking agents, this trust is not the sole contributor to perceived security. Receiving oral confirmation from their remote family members (to whom money is sent) is important to customers but nearly as important is the provision of a valid transaction receipt that can sustain their confidence till the more personal confirmation arrives. Even in terms of the *type* of receipt customers demand, their overall preference for SMS over handwritten receipts, and the security explanation some of them provide for this preference, suggests that their trust in agents has its limits.

There is also an unsettling gap between customers' desire and their awareness about security. The average branchless banking user never completed his schooling, is technology-naive and cannot spot security gaps in the current system. Users believe transaction receipts to be secure for arguably wrong reasons or else, make weak claims about how receipt spoofing is impossible. Securing transaction receipts in branchless banking systems seems to require design from scratch. We began this process in the second part of our research.

5.1 Possible Solutions for Secure Receipts

One obvious solution to the receipt spoofing problem would be to enforce direct interaction between the bank and both the agent *and* the customer during each transaction. For example, if customers are required to call Eko after every transaction request and confirm the transaction details orally (and transactions aborted otherwise), the chance of an agent successfully spoofing a transaction receipt to a customer significantly reduces. However, such a solution may not be sustainable at the scale at which branchless banking systems currently operate: voice calls are more expensive than SMS and USSD and even with an automated solution (based on IVR), the cost of each transaction would be unbearably high. One could consider using SMS or USSD for pull messages (e.g. customer sends SMS message to the bank, bank responds with SMS), but the demand on the network, and the ensuing cost, would still be twice that of the current system.

Another seemingly obvious solution would be to implement a cryptographic signature scheme: have the bank digitally sign each transaction receipt and send both the receipt and the signature over SMS or a data channel. Such a scheme would work only as long as customers' phones are easily programmable with cryptographic software, an assumption that is difficult to make in the developing world. Hundreds of millions of phones in developing countries are still of a "dumb" variety [4] (no programmability without manufacturer support) and even amongst the modern feature phones,there is sufficient platform diversity that a single signature verification program becomes difficulty to deploy for a large customer base [4]. In our own research in the first study, we found that more than 60% users in our interview sample possessed only basic phones (no data connectivity, no available programming tools). A cryptographic solution based on installing software on the SIM card, instead of the phone, is also challenging because it requires co-operation with network operators and a mechanism to ensure cross-operator compatibility.

We thus turn to solutions which embed authenticating information (a la signatures) in transaction receipts but allow customers to *self-verify* such information using their own human capabilities (i.e., without requiring a software program). Message authentication schemes which admit human verification and work for arbitrary digital messages have been proposed in the literature in the past. Two key examples are one-time password based verification [16] and a technique called *visual authentication* [14], which uses cryptographically generated images as a verification tool. However, to the best of our knowledge, none of these approaches have been tested with real users, and never so with branchless banking users. Our study takes a first step in addressing this gap.

5.2 Experiment Design

5.2.1 The Authentication Protocol Used

For our study, we focused on one particular receipt authentication protocol involving one-time passwords (OTPs) which was suggested in [16]. The protocol is simple and involves sharing a sequence of random OTPs between the

sender (the bank server) and the receiver (the branchless banking customer) in a private manner, ensuring that each receiver has a unique sequence. For every transaction receipt m_i that the bank server sends to a customer (via SMS or other methods), it appends a fresh OTP k_i to the message from the sequence corresponding to that customer. The customer's task is to test that k_i is the same as the first "unused" OTP in his own copy of the OTP sequence. The receipt is accepted if and only if this is the case; if not, the customer reports a spoofing attempt to the bank. Once used, an OTP is discarded from the sequence at both ends and the succeeding OTP is used for the next transaction.

OTP-based authentication is a well-established concept and is commonly used in user authentication on the web, the most popular instantiation being RSA SecurID[12]. The key difference in the present setting is that we use OTPs not to authenticate a *human* to a remote computer, but a *computer* to a remote human. From a usability perspective, the task of the human is fundamentally different here: his job is not to enter a fresh OTP into a device correctly, but to view an OTP already displayed on a device (in our case, for example, a mobile phone) and to match it correctly against another password held by him on a different device. We don't know of such a protocol being implemented by any banking system yet.

Devices to store OTP sequences could take different forms: they could be electronic like the RSA SecurID tokens or they could be paper tools, like the codebooks currently used by Eko for user authentication [17]. (For example, in money transfer transactions, agents authenticate themselves to the bank server using their unique codebooks.) Sequence numbers could be used to aid synchronization between the server and the customer; e.g., every time the server sends an OTP to a customer, it attaches an associated sequence number, also printed in the customer's book. Although Eko does not yet provide codebooks to their money transfer customers (they never authenticate themselves to the system), there is a plan to give them booklets during enrolment for keeping transaction records, much like passbooks in traditional systems. Such booklets could potentially be used to carry OTPs in the future.

The above protocol is just one possible technique for receipt authentication and has some security limitations as well (it guarantees security against receipt spoofing, not arbitrary forgeries [16]). Still, we believe it is important to understand the usability of such a protocol before advancing to other more sophisticated solutions. There are more secure protocols one can design using OTPs (e.g., using OTPs to implement pseudo-random functions on messages or using them as graphical keys as done in visual authentication [14]), but none enjoy the simplicity of the above approach.

One could potentially design even simpler protocols involving *fixed* passwords (as opposed to *one-time* passwords) e.g., append a fixed password to every receipt sent to the same customer or use that password for sending other dynamically generated OTPs securely. While fixed passwords enjoy the benefit of not requiring users to carry additional devices, they raise issues around memorability, and also open up the possibility of replay attacks; e.g., if a password is leaked to an agent, spoofing becomes trivial. We thought it prudent to test a system that ensures spoof-resistance against eavesdropping agents.

[12] `http://www.rsa.com/node.aspx?id=1156`

5.2.2 The Experiment

We designed a wizard-of-Oz experiment involving two types of transaction receipts—*basic* and *secure*—implemented in two different mediums—SMS and paper. Our basic SMS receipts had two fields—*amount* and *account number*—the most essential fields for a money transfer transaction. Secure receipts had one additional field called the *secret number*, which represented the OTP. All receipts were timestamped. We avoided including other fields (like TID and agent phone number) in our receipts because findings from our previous study suggested that customers are not consistently attentive towards them and even lack knowledge of some fields like the TID. Since our objective is to understand relative usability of receipts with and without OTPs, we hope that eliminating non-essential fields (besides OTPs) does not affect the qualitative nature of our results.

The choice of paper was motivated by our previous findings (Section 4.3.6), which showed that customers might prefer paper receipts due to their storability and reliability advantages. Paper receipts in our study were essentially printed versions of the SMS receipts, with slightly larger font size. For the secure version of the paper receipts, the intended implementation is to use a networked printing device, one per agent site, that would communicate with the bank server and print transaction details along with the OTPs. We remark that the secure version of the paper receipts is *less* secure than the secure version of the SMS receipts, since the former requires the assumption of a tamper-proof printing device. (If the agent could tamper with the printing device or was allowed to provide hand-written receipts, he could easily spoof receipts.)

We used English for naming fields in our receipts, to be consistent with Eko's receipt system. Each of the three fields, along with values, fit in exactly one line on the experiment phone screen (no word wraps). *Account number* was written as *a/c no.* and *secret number* as *secret no.* We used 6-digit OTPs (generated at random in software) for the secret number, as is standard in other OTP implementations.

Technology. For our SMS conditions, we implemented an automated system for delivering receipts, which included a telephony server (Freeswitch) and an SMS gateway. In the experiments, the researcher would send a trigger SMS from her phone to the server and the server would deliver an SMS receipt to the participant phone. Paper receipts were implemented using pre-printed slips of paper of the size normally produced by point-of-sale devices; we used pre-printed receipts (as against live printing) to simplify experiment setup.

5.3 Participants

We recruited 30 participants for our study. All were Eko customers, who reported to have used Eko's money transfer facility for a range of 3-24 months and conducted at least 2 transactions each. Two overlapped with our sample in the first study. Participation was solicited using the help of 5 agents, who provided us with a list of regular customers, whom we randomly called and invited to volunteer for the study. We focused on money transfer customers since they are the most vulnerable to spoofing attacks in Eko. Participants varied in their backgrounds but with some expected skews. The set included 27 males and 3 females, which is rea-

sonable given our experience from study 1. Only 8 were residents of Delhi, and the rest migrants, again expected. Educational qualifications were low with 11 participants (37%) not having completed 10^{th} grade and 21 (70%) not having made it past high school. Income correlated with education, with 13 participants reportedly earning less than $100 monthly and only 7 participants earning in excess of $200 per month. The age range was 22-61, with a mean of 35.8.

5.4 Procedure

Participants performed 4 types of tasks, one for each condition defined by us—a *within-subjects* design. Each task involved enactment of a money transfer transaction with the participant playing the role of a customer and the researcher that of an agent. A fixed mobile phone was given to each participant for viewing SMS receipts. Before performing each task, every participant was given a slip of paper with an amount X (which varied from Rs. 1000 to Rs. 9000) and an account number Y (fixed for all tasks) and told by the researcher: *"Suppose that you are doing a money transfer of value X into account Y; I will send a message to the bank server and you will get a receipt on your phone."* For paper receipts, the participant was instead told that he would be handed a printed receipt.

Basic Tasks. Each participant did one basic task for each medium, in which he was required to match the amount and account number reflected in the receipt with that provided on the paper slip. Participants read the contents of the receipt aloud and a researcher noted time. Participants then responded with either a 'yes' or a 'no' indicating whether they viewed a match or not. Before doing the actual task, we had the participant practice to ensure that instructions were clear. Multiple practice tasks were done in case of error.

Secure Tasks. For the secure tasks, participants were provided a "secret number card" which contained printed OTPs. Participants were told: *"Suppose this card is given to you and only you by Eko and Eko maintains a copy at the server. Eko will send you receipts containing these secret numbers."* We then defined the notion of a "correct match" to the participants as comprising (a) a match between the amount and account number in an incoming receipt and those in the provided slip of paper and (b) a match between the secret number in the receipt and the *first unused* secret number in the card. (Sequence numbers were provided on the cards.) Participants did three tasks using the same card: they read aloud in the first task (we noted time) and responded with a 'yes' or 'no' indicating whether they viewed a correct match or not. In the remaining two tasks, which were used for estimating accuracy of receipt verification, participants were told not to read aloud and just to indicate correctness of the match. We randomly introduced errors in the secret number in exactly one of these 2 tasks and noted the 'yes'/'no' responses of the participants. The errors were of identical type—swap the 2^{nd} and 4^{th} digits of the 6-digit OTP. As before, practice tasks preceded actual tasks.

While an OTP spoof involving a single swap in the OTP digits has a small chance of occurrence in practice, such a choice helps us estimate the worst-case probability of spoofed OTPs being missed by users. In other words, our experiment estimates an upper bound on the rate at which users would err in detecting spoofed OTPs in practice.

No Security Priming. There was no security briefing about the authentication benefits of the tasks and we did not use the word "secure" at all in our instructions. Instead, we used the term "matching activity" to refer to the secure tasks and "plain activity" for the basic tasks. This helped us study usability independently of security choices and to gauge participants' perceptive understanding of security against spoofing.

Other Details. Tasks were counter-balanced with respect to medium and receipt type[13]. Participant assignment to task orders was random. For each medium, both basic and secure tasks were completed before moving to the next medium. There was a short oral questionnaire (enquiring about user preferences) after completion of each medium and a longer one at the end. A quick literacy test (involving reading a sentence each in English and in Hindi) was also conducted. The study took place "in the field", close to Eko agent shops in 5 well-separated localities of Delhi. Each interview lasted between 30 to 45 minutes. Participants were suitably compensated for their time.

5.5 Results

All participants were able to complete all tasks with evident ease and comfort. In particular, training the participants to do the secure tasks successfully did not take significantly more effort (less than 2 practice tasks, on average) than training them to do the basic tasks. Reading the words *amount* and *secret* from receipts was not consistently easy for participants but proved possible with practice. The lower-educated participants seemed to use presentation order and their familiarity with word sounds as aids: two of them made the mistake of speaking *account* for *secret* and vice versa but rectified the error in subsequent practice tasks.

5.5.1 Viewing Time

As expected, participants took more time to read and match the secure receipts than the basic ones and the time difference was statistically significant for both mediums, as shown in Table 1. While this is not surprising, it is worth noting that secure receipts took roughly twice as long to be viewed as basic ones in our experiment.

5.5.2 Ease of Use

A 7-point Likert scale with labels ranging from *Very Easy* (rated 1) to *Very Difficult* (rated 7) was deployed to measure perceived ease of use on all tasks. Participants consistently reported greater ease of use for the basic tasks. Still, the mean Likert ratings for the secure tasks were encouraging: 2.4 for SMS, 2.2 for paper. No significant differences for ease of use were found across mediums, either for secure or basic tasks. There seemed to be some interaction between medium and receipt type, with SMS becoming less usable than paper for secure tasks; however, we could not quantify interaction effects due to the ordinal nature of our data.

5.5.3 Accuracy

We measured two types of errors made by participants: a *false alarm* wherein a participant reported an incorrect

[13]For receipt type, there was a slight skew in ordering, with more participants doing the secure task first, but this skew was accounted for in the analyses.

Medium type	*Basic*		*Secure*	
	Mean	SD	Mean	SD
SMS	8.23	2.43	15.83	6.63
Paper	7.73	3.0	15.99	7.43

Table 1: Mean receipt viewing times (in seconds) for different tasks ($n = 30$). Viewing time includes time for reading and reporting a match. A 2x2 ANOVA ruled out significant effect of medium on viewing time. Viewing time for secure tasks was significantly greater than for basic tasks across mediums, as confirmed via paired t-tests: SMS ($t(2, 29) = 7.07, p < 0.01$), paper ($t(2, 29) = 6.28, p < 0.01$).

Medium type	*Basic*			*Secure*		
	Mean	SD	Med	Mean	SD	Med
SMS	1.233	0.81	1	2.367	1.24	2
Paper	1.433	0.43	1	2.167	1.65	2

Table 2: Mean and Median Likert scale ratings for different tasks (1=Very Easy, 7=Very Difficult). The Wilcoxon signed-rank test was used to verify significance. Ratings for basic tasks were significantly less, across mediums: SMS ($z = 3.516, p < 0.01$) and paper ($z = 3.7, p < 0.01$).

Medium type	*False Alarm Rate*	*Spoof Miss Rate*
SMS	0.033	0.2
Paper	0	0.2

Table 3: Mean error rates for the two types of errors recorded by us, for both SMS and paper. The spoof miss rates are worst-case estimates.

match between secret numbers even when there was no mistake in the receipt, and a *spoof miss* wherein a participant reported a correct match despite there being a mistake. For each error type, observations were similar across mediums: we observed 1 and 0 false alarms for SMS and paper respectively ($n = 30$) and 6 spoof misses for each. The effect of medium on error rate was statistically insignificant. Two participants made spoof miss errors for both SMS and paper; the rest made errors for at most one medium. Participants without high school education were more prone to making errors than the others, but the gap was not statistically significant.

The rate of spoof misses observed by us ($6/30 = 0.2$) is higher than that of false alarms but is still reasonable, given that it estimates an upper bound on the actual rate. Increasing security awareness about the tasks should help reduce spoof misses further. (Recall that our participants were not security-primed.)

5.5.4 User Preferences

Perhaps the most interesting of our findings were with respect to user preferences. Given that secure tasks were significantly more time-consuming for the participants, that they consistently found them less easy to conduct and that they were uninformed about security implications of either of the tasks, one would expect strong user preference for the basic tasks. In our study, 11 out of 30 of the participants (37%) expressed preference for the secure task and the preference was consistent across mediums. All of these participants attributed their preference to a perceived increase in security. An exemplary quote:

"Matching with secret number guarantees that money has reached the proper place. My faith will increase and my total transactions may also increase."

Participants had trouble articulating their reasons for perceiving greater security in the matching activity, but some gave interesting partial explanations. The most common explanation was that security increased because there were three numbers to be matched instead of two: *"With secret number, there is a third entity to be matched and I can, by matching, figure out if the sent numbers are correct or incorrect. Hence it is better."* While this does not precisely explain the security benefit that OTPs may provide, it is nevertheless interesting to find users who perceive security in a number-matching activity even without receiving information on how and why those numbers are generated. Three out of the eleven participants who chose the secure task over the basic task (27%) attributed their preference to the secrecy of the cards: *"It is more secure since now I have a secret card with secret number which only I know."*

We find these results particularly interesting given the educational and economic backgrounds of our participants and their limited engagement with electronic banking protocols in the real world. A similar study conducted on token based authentication in web banking with more educated users showed a greater bias towards usability [18]; in that study, less than 20% users preferred the most secure task (chip-and-PIN authentication) over other more efficient and less secure tasks. In our study, we found no significant effect of literacy or education on user preferences for the individual tasks. In fact, 4 out of the 11 participants who were schooled only till 8th grade expressed a preference for the secure task. Overall, 19 out of 30 (63%) rated the secure task as being more secure (security ratings were solicited *after* collecting all preference data, to reduce bias); 5 out of the 11 eighth-grade dropouts in school (45%) reported this rating, while 3 out of the 9 graduates (33%) did not.

When asked whether making the use of the secret cards mandatory would affect their usage of Eko, only 6 participants responded 'yes'; 5 of these claimed that their usage would *increase* and the last one said *"It may decrease since I may forget to bring the card."* When asked whether and how much they would be willing to pay for each card, 21 participants responded favorably; 20 gave values in the range of \$0.2 to \$2 per card, averaged \$0.7, while one said "Anything!" Nine were unwilling to pay. This essentially reduces to an average pledge of \$0.53 per OTP card and, since our cards contained 10 OTPs each, to roughly 5 cents per OTP. This is quite encouraging given that OTPs would introduce a negligible bandwidth overhead in a real implementation.

However, overall preferences of participants were still in favor of basic receipts. Participants justified this based on some obvious failings of the counterpart: *"[Matching activity] takes more time; I come to Eko mainly because it saves me time"*; *"[Comparing] amount and account only gives me more comfort"*; *"It will be a hassle to take care of the card."* One of the participants explained his preference for basic

tasks based on his existing faith in the receipt system: *"For people who do not believe in the receipts, [the matching activity] is more secure, but for me, there is no advantage."*

In terms of their general preference for the medium to view transaction receipts in, preferences were aligned with our findings from the previous study: 17 out of 30 participants (57%) preferred SMS over paper. The reasons participants gave for their choices were similar: storability being the main advantage cited for SMS and readability for paper.

5.6 Limitations

While our experiment provided us some insight on how users of branchless banking systems may use token-based receipt verification schemes in practice, we view it only as a preliminary exercise in this investigation. We point out some limitations here. First, we adopted convenience sampling to recruit participants and relied on information provided by agents in the process. This made our study easy to conduct, but it also limits generalizability. Second, we used a simplified version of transaction receipts to ease participant training. It is unclear whether adding more fields could have affected results positively or negatively, but it is clear that increasing the readability of the current SMS receipts of Eko is desirable, given users' feedback from the first study. Third, our study did not evaluate the effect of security training on user preferences (although this also helped us get interesting data on what lack of training accomplishes). There is literature which suggests that training can tilt user preferences towards more secure tasks, at least within the context of usability studies [10]. Finally, we did not evaluate longitudinal effects. If the OTPs are deployed in practice, would they be actively used for receipt checking? We believe this will vary across users and across transaction values but given the security responsiveness we have seen in users in our studies, it is plausible that the practice will be used by some (if not all) of them.

6. DISCUSSION

User studies that examine security preferences of people in the developing world are rare and it is only natural to expect that the less-educated and less-literate of the world have a poor perceived understanding of security or at least, low ability to tell secure and insecure interfaces apart. Our findings suggest that this may not necessarily be the case. Even without being security-primed and even after consistently reporting that the secure interface is less usable, more than a third of the participants in our second study chose the secure option because it appeared more secure to them. Several of these never completed their formal education and still face reading difficulties. These findings are consistent with another study [17], also conducted with branchless banking users, which found multiple examples of educationally poor people who possessed a non-trivial understanding of security issues in PIN-based authentication, even without security trainings.

There is an interesting contrast between what we found in the two studies reported here. While less than 10% of the users in our first study were aware that Eko receipts are spoofable (the rest being unaware and content), more than 60% in the second one demonstrated the ability to differentiate spoof-resistant receipts from the spoofable ones, and 37% stated a preference for the former. None of the 6 security-aware users in study 1 participated in the second study. It is clear that distinguishing between secure and insecure UIs comes more easily to users than identifying weaknesses in a stand-alone insecure one. Furthermore, our research suggests that branchless banking users trade off security for usability differently than users of certain elecronic banking systems [18], which is a premise worthy of further exploration.

Finally, it is also apparent that the majority of branchless banking users will not give up convenience for security, as is the usual finding in research and practice. The average user tends to treat security as an externality [9] and even the most educated and informed perceive security tools as annoying, particularly if the immediate security benefits cannot justify the usability burden [7]. Such a belief may prevail amongst branchless banking users although here, the cost-benefit ratio of executing diligent receipt verification seems low, given the universal desire for security in financial transactions, the weaknesses in the current systems and the ease with which some types of receipt verification (e.g., OTP-based verification, as studied here) can be carried out. In a real deployment, providing the users with the flexibility to choose between secure and insecure options (OTP card vs. no OTP card) with a clear explanation of associated trade-offs will likely prove most practical.

7. CONCLUSION

As people living in the developing world get exposed to new and efficient ways of managing money, their exposure to theft and exploitation may also increase. In this paper, we considered one pressing security problem—the spoofing of transaction receipts—in the context of branchless banking, a modern mechanism to facilitate finance in developing regions. This is a problem that has led to exploitation of multiple users in recent events. We studied current practice amongst users of an actively-used system named Eko in India and found both a universal desire for reliable and dependable transaction receipts as well as a tendency to excessively trust human agents and to over-rate the security offerings of current systems. We explored the usability of a simple, one-time password based protocol for receipt verification to address the spoofing concern, tested it with 30 users, and found that several users in our sample, despite limited formal education, were able to identify this protocol as being more secure than current practice. Over a third of the users stated a preference for using the protocol, even with the evident usability degradation. Future work will compare the security and usability of this protocol against other alternatives, study questions around incentives and user choice in the deployment of receipt verification protocols and attempt to put some of this research into practice in collaboration with service providers.

8. ACKNOWLEDGMENTS

Thanks to Anupam Varghese and his colleagues from Eko in supporting us during the studies. Thanks also to students in the PreCog team of IIIT Delhi for feedback.

9. REFERENCES

[1] Eko India Financial Services Pvt. Ltd. `http://www.eko.co.in`, 2007.

[2] M-Pesa. http://www.safaricom.co.ke/index.php?id=257, 2007.

[3] SMSSpoofing: Everything you ever wanted to know about SMS spoofing. http://www.smsspoofing.com, 2008.

[4] Global mobile statistics 2012. http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats, 2012.

[5] Y. Ben-David, S. Hasan, J. Pal, M. Vallentin, S. Panjwani, J. Chen, P. Gutheim, and E. Brewer. Computing security in the developing world: A case for multidisciplinary research. In *Proc. of NSDR*. ACM, June 2011.

[6] P. Bhattacharya and W. Thies. Computer viruses in urban Indian telecenters: Characterizing an unsolved problem. In *Proc. of NSDR*. ACM, June 2011.

[7] A. J. Dewitt and J. Kuljis. Aligning usability and security: a usability study of Polaris. In *Proc. of SOUPS*. ACM, July 2006.

[8] GMeltdown. Tribulations of the M-Pesa agent. http://www.gmeltdown.com/2010/11/tribulations-of-m-pesa-agent.html, Nov. 2010.

[9] C. Herley. So long and no thanks for the externalities: The rational rejection of security advice by users. In *Proc. of NSPW*. ACM, Sept. 2009.

[10] I. Ion, M. Langheinrich, P. Kumaraguru, and S. Capkun. Influence of user perception, security needs, and social factors on device pairing method choices. In *Proc. of SOUPS*. ACM, July 2010.

[11] D. Kumar, D. Martin, and J. O'Neill. The times they are a-changin': Mobile payments in india. In *Proc. of CHI*. ACM, May 2011.

[12] C. McKay and M. Pickens. Branchless banking 2010: Who's Served? At What Price? What's Next? *CGAP Focus Note*, 66, Sept. 2010.

[13] I. Medhi, S. N. N. Gautama, and K. Toyama. A comparison of mobile money-transfer UIs for non-literate and semi-literate users. In *Proc. of CHI*. ACM, May 2009.

[14] M. Naor and B. Pinkas. Visual authentication and idenitification. In *Proc. of CRYPTO*. Springer-Verlag, Aug. 1997.

[15] M. Paik. Stragglers of the herd get eaten: Security concerns for GSM mobile banking applications. In *Proc. of HotMobile '10*. ACM, Feb. 2010.

[16] S. Panjwani. Towards end-to-end security in branchless banking systems. In *Proc. of HotMobile '11*. ACM, Mar. 2011.

[17] S. Panjwani and E. Cutrell. Usably secure, low-cost authentication for mobile banking. In *Proc. of SOUPS*. ACM, July 2010.

[18] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers and Security*, 28(1), 2009.