Card3000

Ajay Alfred,
Shawn Callegari,
Mike Hotan,
Ravi Pinjala

Contents

1. Problem and Solution Overview
2. Contextual inquiry Participants
3. Contextual inquiry Results
    a. Availability and Awareness
    b. Incentives
    c. Usability / Digestibility
    d. Security / Accountability
4. Task analysis questions
5. Three tasks
    a. Task 1 - Making a quick payment (Easy)
    b. Task 2 - Dealing with an overdraft on the payment card (Medium)
    c. Task 3 - Reporting fraudulent transactions (Hard)
6. Storyboards for our initial designs
    a. Design 1
    b. Design 2
    c. Design 3
7. Selected Interface Design
    a. Reasoning
    b. Functionality summary
    c. User interface description
8. Three scenarios corresponding to tasks

Problem and Solution Overview

When you think about it, credit cards are pretty terrible. They are horribly insecure, requiring no authentication at all to use. What little security they have is completely reactive - if you or your credit card company notices that something is amiss, you can cancel the card, hopefully before too much damage has been done. We should expect better from something that's tied to our bank accounts! On the other hand, credit cards also have some advantages: people are familiar with how they work, they're really simple to use, and they're easy to carry around.

We would like to propose something new, which maintains the positive aspects of credit cards, but dramatically improves their security and flexibility. Our Card3000 system is a hardware platform for software-defined credit cards, which keeps the same form factor as plastic credit cards, and maintains compatibility with magnetic stripe readers. The hardware may be a bit beyond what can be manufactured today, but when you look at current hardware trends, it's entirely possible that it could be built within the next decade.

Contextual inquiry Participants

Vi is a college student in her early 30's. Although she is an avid bargain shopper, she does not use her phone to make in store mobile payments. She approaches in-store payments from a more traditional standpoint. She uses credit cards to make larger purchases because she feels that it is necessary to have some form of accountability post purchase. She maintains a credit card and debit card in her wallet for her day to day activities. She is very conscious about maintaining a conservative spending behavior. She would like faster access to security and accountability details about her credit accounts after a purchase.

Ian is in his mid 20's, and is a software engineer. He has moved into a new household and has been recently making more in store purchases. He usually shops online because he likes to reference reviews. Because he is shopping for physical content that he looks to place in his home, he appreciates the ability to view items in store and purchase items without having to pay daunting shipping cost. Whether it be online or in store, Ian appreciates the ability to apply royalty benefits per purchase. Ian is also very aware of the security vulnerabilities of modern magnetic stripe credit cards. Despite the awareness, he decides to continue to use his credit cards in trusted establishments.

Craig is a 25 year old Electrical Engineer working for a robotics company. He is a gadget enthusiast, and is always up-to-date with the latest technology. He is also a minimalist and tries to reduce the clutter in his life. Craig would love to reduce the number of cards he carries in his wallet by moving to an all digital wallet system, but he carries an iPhone which does not support NFC payments. He does use his phone wherever possible, to store loyalty cards and membership numbers, and passwords. Fortunately, Starbucks has a mobile payment solution that works well on Craig's iPhone, which means one less card in his wallet. He uses the app for all Starbucks purchases, and he enjoys the fact that he can also check his balance and top it up as needed.

Contextual inquiry Results

Availability and Awareness

There are many different kinds of in store payment options. There are so many that it is difficult for merchants to support all of them. It is also too difficult for consumers understand when and where to use these specialized systems. Vi and Ian are both interested in making mobile payment their priority payment method. They are both looking for a more secure payment system. The main issue they brought up was that most merchants either didn't support such systems or do not know they supported such systems. For example, while conducting our contextual inquiry with Vi, the cashiers at McDonalds had no idea that customers could pay with NFC. Vi does not actively look for these non traditional payment systems. Ian is actively engaged with new technology and looks for these locations. However, Ian is constrained by his smartphone. His phone is too troublesome to set up for non traditional mobile payment systems.

On the other hand, Craig does everything he can to avoid carrying credit cards. He wishes that more stores used mobile payment options. Craig uses the Starbucks mobile application to make mobile payments. This constrains him to only be able to make payments with Starbucks. Associating a mobile application to the merchant that produced the application ensures that the payment method exist. However, having every merchant have their own application is extremely cumbersome for consumers. Our participants, with the exception of Craig, were more likely to resort to traditional payment methods than to add another application to their smartphone. The lack of availability and standardization has deterred a majority of our participants from using non traditional payment systems.

Incentives

Craig demonstrated how Starbucks incorporates a loyalty program within the application itself. Craig was able link credit cards and preloaded Starbucks cards. This allowed him to earn credit for every purchase. The Starbucks process is relatively simple, Craig was able to easily open the application and show a barcode to pay. Craig appreciates how the application automatically linked to his Starbucks account, seamlessly updated his royalty status.

Vi and Ian both used NFC based service to make payments. Ian pointed out that NFC did not provide any incentive that relates to royalty accounts. They both carry as few cards as possible in order to avoid running up a lot of credit card debt. They were pleased with the ability to switch between accounts without worrying about which card to leave at home. It was obvious that a smartphone's ability to store and manipulate data can be highly beneficial for both consumers and merchants. Our participants all would like pervasive integration of loyalty programs and promotional accounts into every

purchase they make. Credit cards are static, therefore they can only provide incentives that tie directly to the credit card itself. Our participants want to see incentives that tie directly to merchants.

Usability / Digestibility

For all three participants the functionality of paying with credit cards was instinctive. All three are able to pay with physical credit cards almost effortlessly. Credit cards have become a modern day essential for making impulsive or relatively large payments. Vi and Ian both expressed that a reason they continue to use physical credit cards is that they understand the entire transaction. Even though both of them didn't necessarily like physical cards, it was just the most convenient. Craig was clear that even though he knew how to use plastic credit cards he did everything in his power to use his smartphone.

A key difference we found was in the variations of representations between mobile and credit cards. Credit cards vary minutely compared to the interfaces that are presented on mobile payment systems. Mobile interfaces vary relatively greatly depending on the application and operating system. Ian and Craig were both technical savvy, therefore learning new user interfaces is not as much of a hinderance as it is for Vi. Initially, she had no idea when her phone was ready for the NFC transaction. Google Wallet's interface was relatively simple, but it was difficult for a non experienced user to learn when to tap to pay. This presents a common problem that is arising out of the prominence of different types of payment methods. The variation of interfaces makes non traditional payment systems less approachable.

Security / Accountability

Ian and Vi both had concerns about credit security. Ian is very aware of the vulnerabilities of modern day magnetic strips and credit card numbers. Vi is generally aware of these vulnerabilities. Craig was not concerned at all. Craig was comfortable with the credit card companies ability to insure false transactions. The concern over security varied through our participants.

However, all the participants were concerned with some level of accountability. Ian collects receipts for tax purposes. Vi collects receipts for strict accountability purposes. Craig collects receipts when he might need to return something. All of them check their transaction history at least once a week. This shows that there is a desire for real time assurance and credit awareness.

Task analysis questions

1. Who is going to use the system?

Everybody who currently uses a credit card could benefit from our system. This covers most people these days, since credit cards are widely used. Our system would not be used by people who pay for things with cash.

2. What tasks do they now perform?

Overwhelmingly, the most common task people perform with credit cards is the simple payment scenario - handing their card to a cashier, and having the cashier ring up a purchase. Online purchases are also common these days, and those should be treated as a distinct task, since the workflow is very different. Less common tasks covered by our system are looking at transactions, which people normally do through their bank, and securing a card, which is normally done by calling the credit card company on the phone.

3. What tasks are desired?

People want to be able to pay for things, fundamentally. Beyond that, they want the process to go smoothly (without having to think too much), they want everything to happen quickly, and they want the protocols involved to be secure. They also want to have the option to receive receipts, for scenarios where they later decide that they want to return an item and need proof that they purchased it, but in most cases receipts aren't desired.

4. How are the tasks learned?

Paying for things with a credit card is a pretty fundamental life skill, so people usually learn it from their parents as they're growing up.

5. Where are the tasks performed?

People pay for things in a variety of ways - in stores and restaurants, online, through the mail, and even over the phone occasionally.

6. What's the relationship between customer & data?

There are three parties involved in a transaction: the buyer, the seller, and the buyer's bank. And there are two classes of data: Information about the customer's account, and information about the individual purchases. Account data is jointly owned by the buyer and the buyer's bank, and both have full access to that data. The seller has limited access to that data, since they need to be able to request payments and verify the customer's remaining balance. Transaction records are owned by the bank (and also

tracked by the seller), and visible to all parties. Neither class of data should be visible to anybody outside of a given transaction; both account information and transaction records must remain private by default.

7. What other tools does the customer have?

Aside from credit cards, cash is another option for paying for things. Cash is different in that it carries value directly, instead of being tied to an account. This leads to very different security properties: cash makes identity theft impossible, because there's no account to compromise, but direct theft is much more of a problem, because there's no equivalent to canceling a lost credit card. It's also clumsier to use to actually pay for things, since making exact change is a manual process. Finally, cash is anonymous, which is important to some people, while credit cards are implicitly tracked by several parties.

8. How do customers communicate with each other?

Customers don't generally use these systems to communicate with each other, but they do communicate with cashiers.

9. How often are the tasks performed?

The exact frequency varies a lot between customers, but it's not uncommon for people to make several purchases per day.

10. What are the time constraints on the tasks?

Purchases need to be completed as quickly as possible, usually on the order of 15-30 seconds. It also needs to be possible to complete the task with very little cognitive load, since in some situations like a grocery store checkout line, both parties to the transaction will be doing other things at the same time.

11. What happens when things go wrong?

There are all kinds of things that can go wrong:
- At the point of sale, if the user has insufficient funds, the transaction will be rejected. The user can fall back to a different payment method.
- If the user loses their card, they will need to cancel it by calling their credit card company. The company sends them a new card, with a different number, and the user receives it a few days later. Until then, they are stuck without a card.
- If the user's account information is stolen, the consequences are mostly the same as loss, plus the thief

can use that information to make fraudulent purchases. Either the user or their credit card company will eventually notice this, and cancel the card.
- Without a network connection, no credit card payments can be made. Cashiers can process payments over the phone, or customers can use cash or other payment methods.

Three tasks

Task 1 - Making a quick payment (Easy)

Shopping has become an integral part of our lives, and so has carrying multiple payment cards. With each retailer and financial institution running its own rewards program, the need to carry a bunch of cards has not helped solve the problem. The checkout process often consists of juggling between multiple cards to ensure that you earn those precious reward points and pay with a card that has the best rewards program. We believe making a payment shouldn't be this tedious.

With Card3000, a customer can use a single card for all their payments and reward programs. The first task is a testament to just how easy the whole payment process can be. A customer walks up to the checkout counter to make a payment using Card3000. The card is activated through a biometric signature and the customer is prompted to activate the card for payment.

Task 2 - Dealing with an overdraft on the payment card (Medium)

Running into an overdraft while making a payment can be embarrassing. And that probably happens because payment cards today are static and unhelpful with relaying important information that can avoid such situations. Card holders generally have to keep a mental note of how much they can spend on their card and the problem gets worse with multiple card accounts. Keeping a track of the amount spent and spending limit on each card often involves logging into multiple online web portal to check these details which makes the whole process even more convoluted.

With Card3000, all this information is available on the card when you need it most. A customer can check the spending limit for each card through the simple and intuitive gestures of Card3000. This task will involve changing the payment method to a different card account since the default card has reached its spending limit.

Task 3 - Reporting fraudulent transactions (Hard)

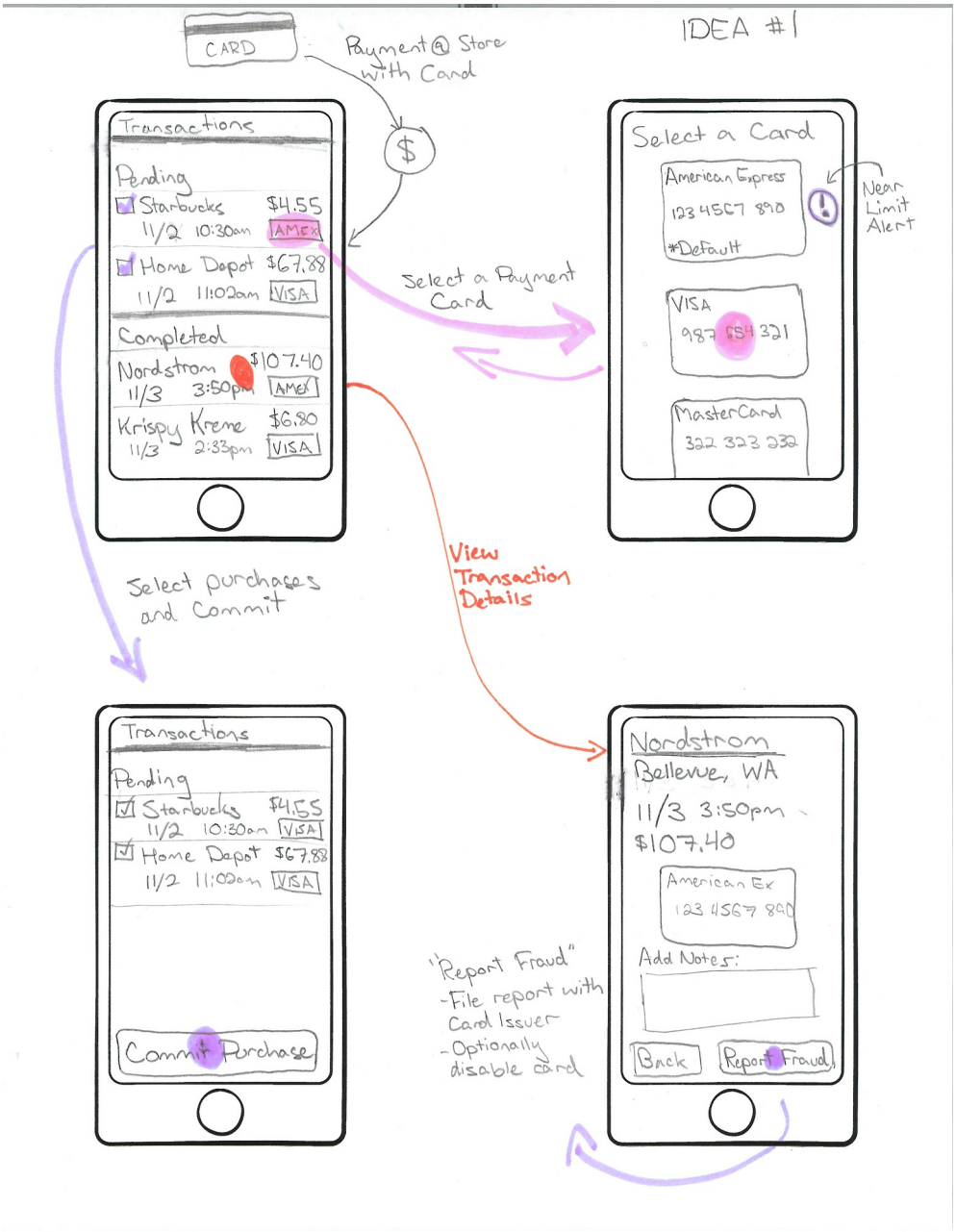
Fraudulent transactions happen all the time, and while there's only so much security that can be built into the system, catching and reporting such transactions as early as possible can bring us a step closer to preventing financial loss. Currently, the only way to identify if a card has been misused is through the online web portal or mobile apps that most financial institutions provide. Accessing a list of card transactions through them still involves a few too many steps that deters their frequent use. The result being that fraudulent transactions often go unnoticed until its too late.

With Card3000, all this information if available at your fingertips. This task involves making an payment and then looking through a list of card transactions using the intuitive interface of Card3000. If any fraudulent transactions are found, the cardholder can immediately report them to the bank and even block the card for payments. After the bank has blocked the old card and sent a new card, the customer must add and activate the new card on Card3000.

Storyboards for our initial designs

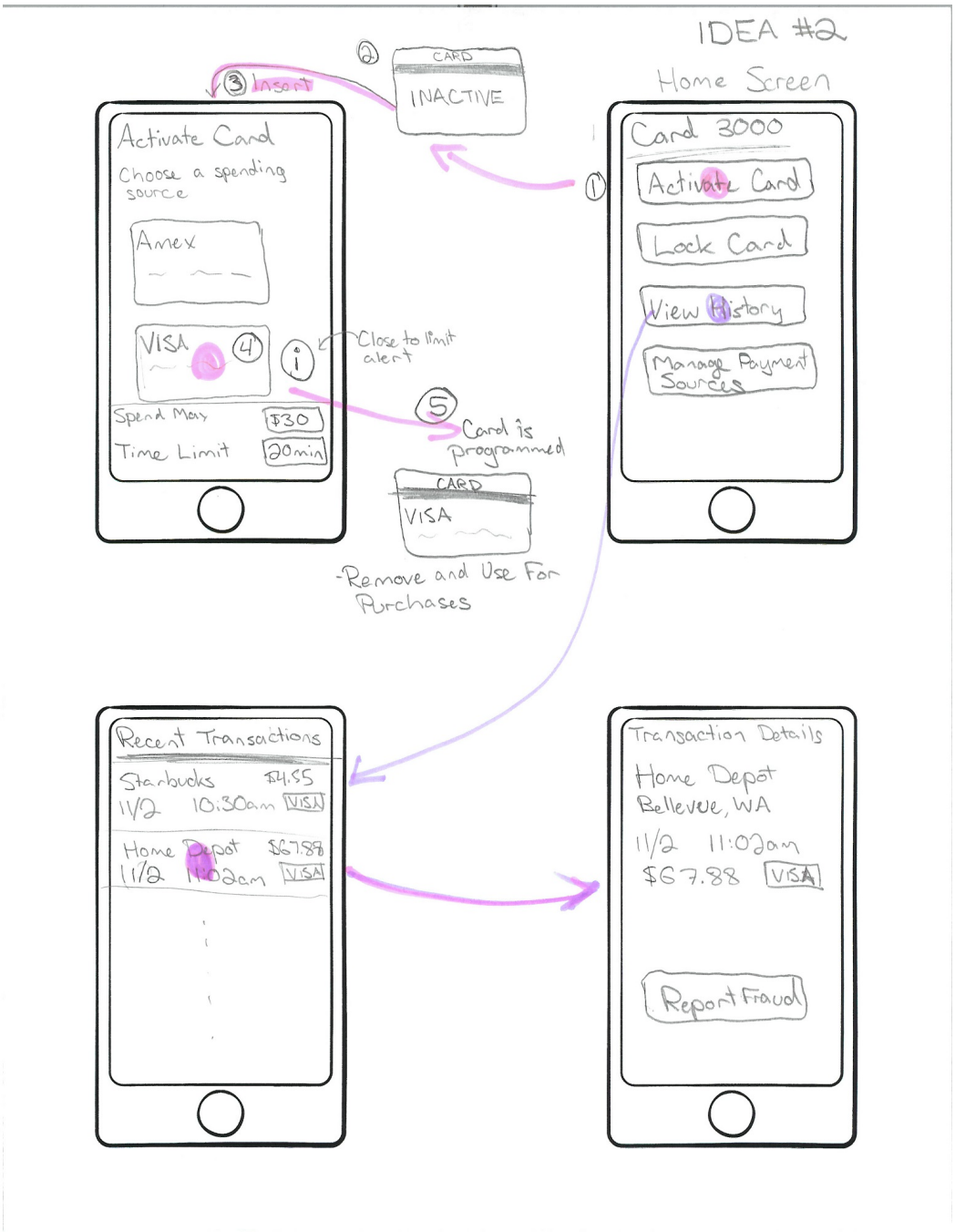
Design 1

A standard magnetic stripe card, with an accompanying back end service and smartphone app. User pays for purchases using the single card, and then uses the app to choose which credit card each transaction is charged to. If no selection is made within a time limit (i.e. 6 hours), the purchase is charged to the default card.



Design 2

A programmable magnetic stripe card with an accompanying smartphone app. The card is normally in an inactive state, and cannot be used for purchases. The user activates the card by selecting a payment credit card on their smartphone, and holding it near the card. This enables the magnetic stripe and allows the user to make purchases with it as though it were a standard card.



Design 3

A smart card containing all the logic and security within a device the size of a credit card. This design includes a programmable magnetic stripe, an NFC chip, and can display linear/2D barcodes, so all modern payment standards are covered. Interactions are done solely through the card's touchscreen interface (no phone or other device needed).

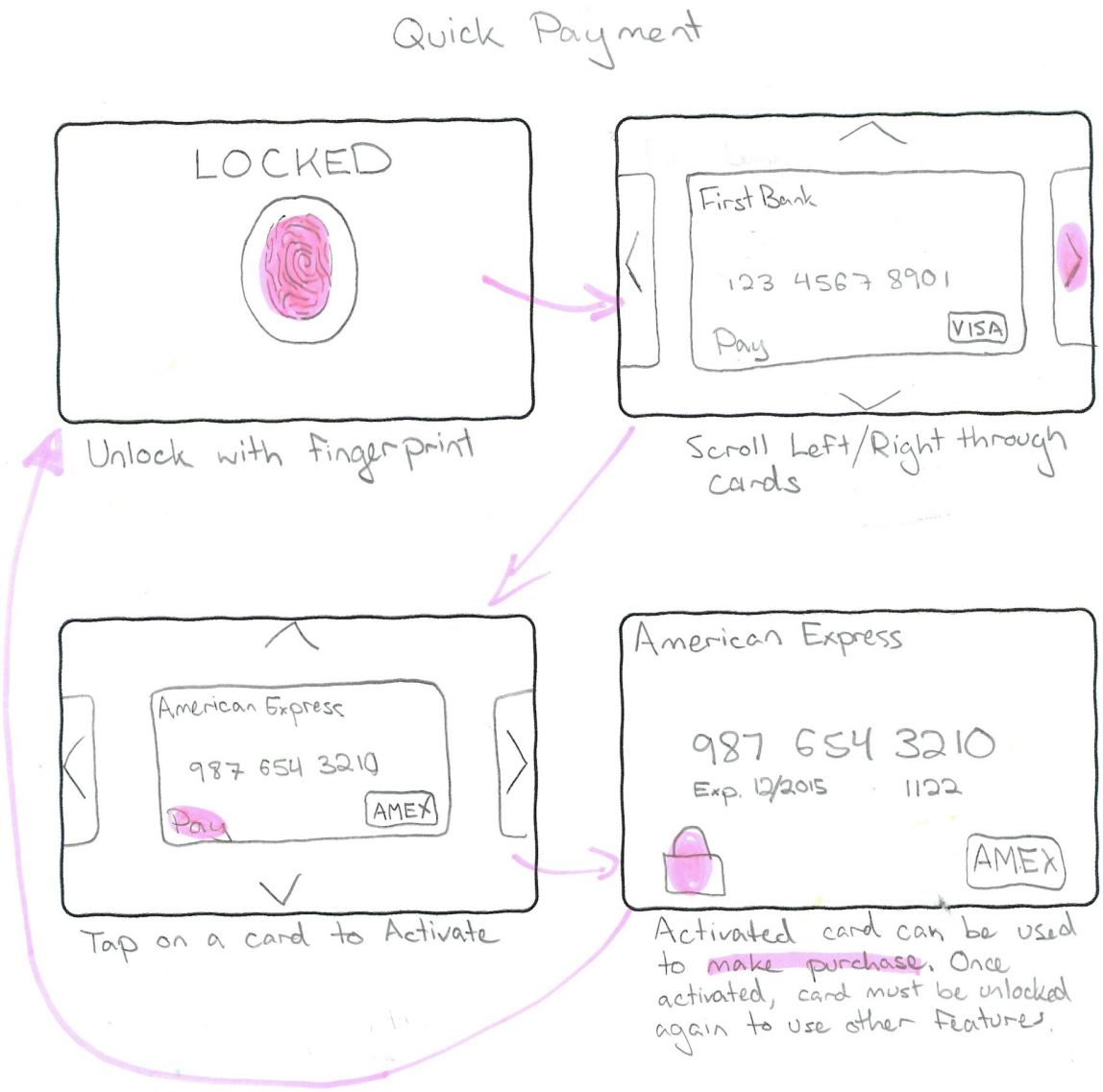


Image 8.3.1 - Quick Payment. Steps for making a payment using the Card3000, beginning with the locked state and ending in an activated card ready to be used for payment.

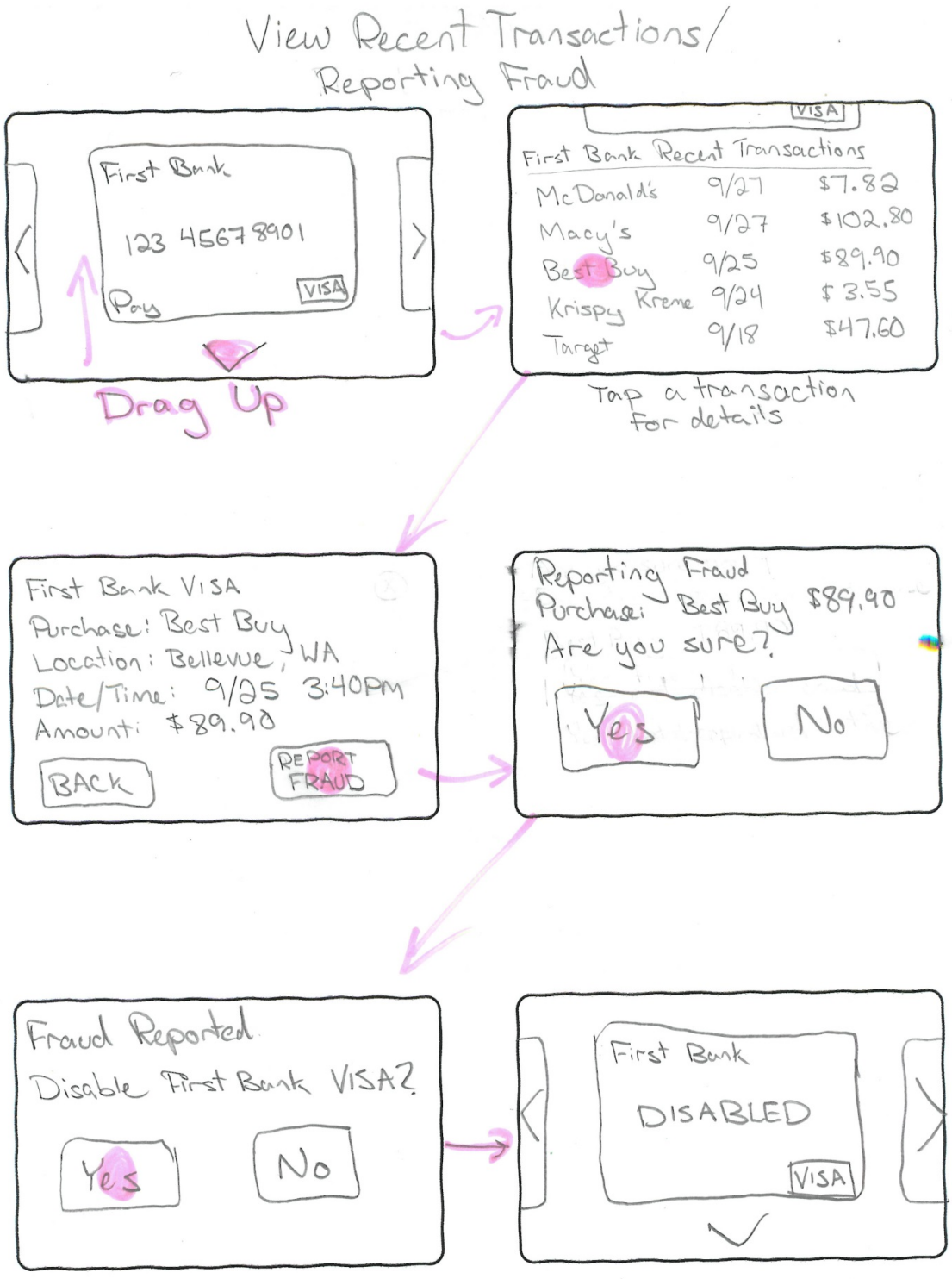


Image 8.3.2 - View Recent Transactions & Reporting Fraud.

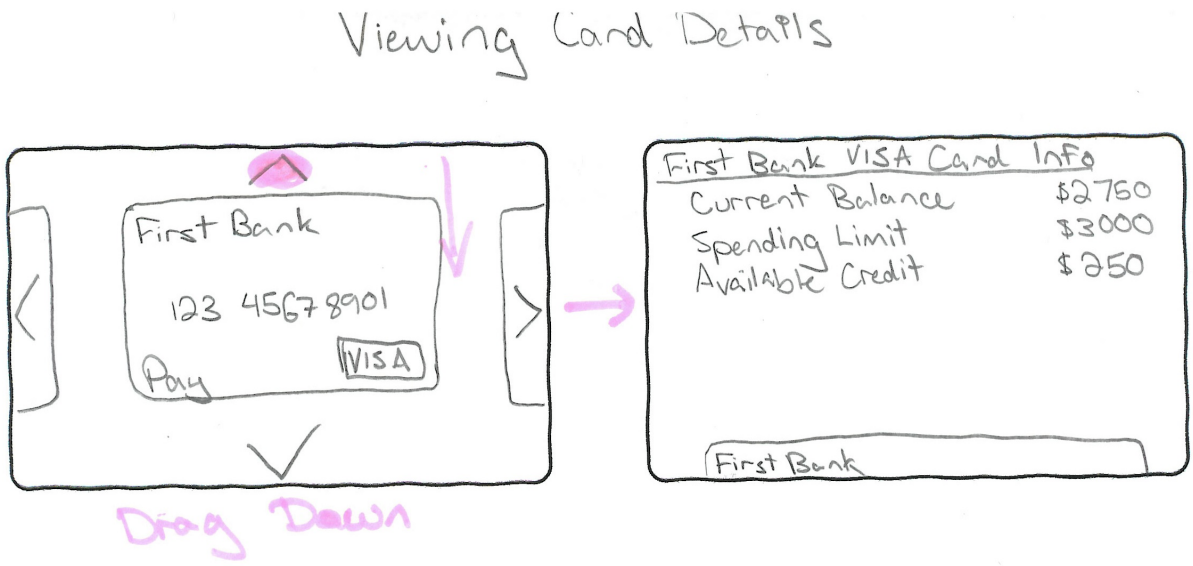


Image 8.3.3 - Viewing Card Details. Displays additional card details, including the spending limit and available credit.

Selected Interface Design

Our final decision is design three but incorporates some benefits from one and two. All three models are represented as a cohesive balance between mobile technology and a physical credit card. They differentiate from each other with how the balance of capability is distributed between the two payment mediums. We decided on interface design three. Design three uses a single transaction medium, the "smart" credit card:

- The card itself will be touch enabled.
    - Users can swipe left and right to switch between cards
    - Users can swipe up and down to see account details about the last visible credit account
- Card will be secure and "private enough"
    - Traditional physical cards have vulnerabilities. These cards display all the content all the time. Once an adversary obtains a consumer's card, they are free to extract the data and make fraudulent charges. This results in the burden of cancelling accounts after losing credit cards. Also, consumers frequently hand over physical cards to merchants. Consumers are left with conducting transactions
    - Card3000 will biometric authenticated and no data will be shown prior to authentication
    - Card 3000 will have an ability to hide non pertinent data when merchants handle consumer cards
- Card will not require wireless connection

    - Mobile phones rely on data connectivity. This card will function with and without wireless connection.
- Display pertinent information
    - See recent transactions in real time
    - Link to receipts

Reasoning

We recognize a couple major reasons why mobile payments has not become pervasive. One is that it is not ubiquitously available. Currently, consumers have to go out of there way to purchase the phone with correct capabilities and download additional applications. This is a complication and deterrence. Card3000 utilizes the same payment medium that consumers are familiar with. Subsequently, merchants would be able to continue to use their current payment infrastructures.

Creating an interface on a physical credit card allows us leverage its familiarity. Using a physical card allows us to create a more digestible interface. We will design a smart interface utilizing common features found in physical cards. This allows users to view a familiar visual interface and conduct the same physical transaction.

We also chose our payment medium for its simplicity. The other designs had more dependency. Having a programmable card and a smartphone requires both to work properly. Having a mobile application that relies on a cloud service requires both to work properly. We force consumers to rely on external dependencies. We want Card3000 to feel assuring and reliable to consumers. Therefore choosing the interface with the least moving parts provides the most comfortable experience.

Functionality summary

Card3000 is a smart card that replaces and functions like all the other payment cards a person may own. It includes a salient set of features that address multiple aspects of security, convenience and accountability.

Authentication

Being a one-stop payment instrument that has access to all the financial accounts mandates the need for a strong authentication mechanism. Card3000 implements a biometric authorization mechanism that is easy to use and secure at the same time. In order to access any of the card account details or to activate the card for payment, the user must be identified by scanning their fingerprint. Card3000 only works for

the account holder and this is ensured by requiring a fingerprint scan at the start of each session. The card will auto-lock after a set time period of inactivity or if the user explicitly locks the card.

Activating the card for payment

After authenticating the card holder, Card3000 displays the card details of the default payment card. The user can swipe through a list of card accounts on Card3000 as well. In order to make a payment, the user must select and activate a card for payment. This is done by swiping down on the selected card to reveal the card activation interface.

After activating the card for payment, the interface displays details of the payment method such as card number, cardholder name, etc. (as found on conventional cards today). Additional card account details are unavailable once a card has been activated for payment since making a payment sometimes involves handing over the card to the cashier to complete the transaction and to avoid revealing sensitive account information to unauthorized users, the card is put into a active, but locked state. The cardholder must be authenticated (through a fingerprint scan) again to access transaction and account details.

Accessing multiple card accounts

Card3000 supports the use of multiple card accounts. Accessing the details of a different payment card is as simple as swiping left or right on the interface to switch to another card account.

Accessing card transactions

After selecting a particular card account, swiping up will reveal the latest transactions that have been made with that card. A list of 5 of the latest transactions is displayed on the interface. Clicking on a transaction will show details associated with that transaction such as amount, merchant, transaction date, approval status, and options to report a fraudulent transaction.

Reporting a fraudulent transaction

If the card holder notices a fraudulent transaction, it can be reported by selecting transaction details and clicking the ‘report fraud’ button. This brings up an agreement notice and an action to report the transaction to the bank. The interface also displays options to immediately block the account for further use.

User interface description

Step 1 - Authentication

The cardholder must authenticate himself by scanning his fingerprint through the authentication screen on Card3000. This is the first step to gain access to all other features on the card. The interface of the card displays an image of a fingerprint in portrait mode (Image 8.3.1 Top-Left). The card holder places his thumb on the card to authenticate. The system scans the fingerprint and if it identifies the user, it changes the interface to display the default payment card details.

Step 2 - Select payment card

By default, Card3000 displays the default payment card details after authentication. This includes the card name, card number, exp. date, account holder name, and payment networks (VISA,MC, AMEX, Discover, etc). There's also an arrow on either side of the card to denote that swiping on the interface will bring up the next card account (Image 8.3.1 Top-Right).

Step 3 - Activating a card for payment

In order to activate the card for payment, the user swipes down on the selected payment card. This brings up the card activation screen. The user clicks on the button 'Activate for Pay' (Image 8.3.1 Bottom-Left). The card interface changes to display the card details as described in Step 2. It also shows a small lock icon at the top right corner to indicate that the card is in payment mode but has been locked to avoid showing sensitive account information (Image 8.3.1 Bottom-Right). The user can now hand over the card to the cashier to complete the payment. Clicking on the lock icon takes the user back to Step 1 to ensure authentication before showing any additional card information.

Step 4 - View card transactions

To view the transactions of a particular card, the user first selects the particular card by swiping left/right. A swipe on the card towards the top brings up a list of transactions. The interface shows 5 of the latest transactions that were made with that card (Image 8.3.2 Top-Right). To go back to the card details, the user can swipe down on the screen which will bring back the list of card accounts.

Step 5 - Transaction Details

To view transaction details, the user clicks on the transaction to view additional details. The card interface changes to display details such as the merchant name, transaction amount, date & time of the transaction, bank approval status and options to report a fraudulent transaction (Image 8.3.2 Center-Left).

Step 6 - Report a fraudulent transaction

To report a fraudulent transaction, the user clicks on the ‘Report Fraud’ button. This changes the interface to display a notice of the legal agreement required while reporting the fraud (Image 8.3.2 Center-Right).

The user agrees and clicks on the ‘Report’ button. After reporting, the interface also displays a popup that allows the user to block the card from further use (Image 8.3.2 Bottom).

Three scenarios corresponding to tasks

Scenario 1 – Making a quick payment

Jason is always on the go. He travels a lot for work, and uses several cards for different purposes; he has a company credit card, and several personal cards with various benefits. He likes to book his travel on an airline card to accumulate air miles, and he pays for gas using a special card that offers 3% cash back on all fuel purchases. Keeping all these cards straight is problematic, but carrying them all would be just annoying. Instead, Jason leaves the cards and home and carries his Card3000, which gives him access to all these cards in one small package. When sitting at the office and booking a flight, he pulls out his Card3000 and flips through the interface to reveal his airline card. He reads the number off the card and enters it into the booking site. Once on the way, he wants to pay for snacks at an airport. He pulls out his Card3000, cycles through the registered payment methods, and chooses his company card. Once activated, he uses it as though it were a normal credit card, swiping it through the payment terminal. Once at his destination, he needs to top up his rental car. He pulls up to a gas station, chooses the gas rewards card on his Card3000, inserts it into the pump, and pays for fuel as he would with a normal card. With the Card3000 in his pocket, Jason has access to all of his payment methods in one convenient device, and there's no need to haul around a wallet full of cards.

Scenario 2 – Overdraft protection

Susan is a shop-a-holic. She keeps a few active credit cards, and often rings them up close to their limits. Every so often, as she's nearing the month's end, she accidentally overspends on a given card and it is declined at the store. This is a humiliating situation – nobody likes to be told their card is declined, and be forced to find another payment method on the spot. Recently, Susan traded her physical cards for a Card3000. Now, as is about to make a purchase at the department, she unlocks the Card3000, looks at the details of her default card, and checks its balance. If the card is too close to its limit, she can choose another one. This gives her the peace of mind of knowing that her card won't be declined, and it also helps to keep her on top of her spending habits by increasing her financial awareness.

Scenario 3 – Card Security

Kevin likes the benefits of credit cards (convenience, rewards, etc), but he really doesn't trust them. He has a few cards, though he rarely carries them as he believes that they're an inherently insecure liability. Instead, he typically carries cash and a debit card. Kevin's new Card3000 may finally be the answer! His cards are now securely stored within the device, and can only be activated with his fingerprint. When he's about to make a purchase, Kevin unlocks the Card3000 by placing his finger on the sensor.

He is recognized as the card's sole user and it unlocks the interface. He selects a payment card and then taps the 'Activate for Pay' option. This place the Card3000 into a mode such that it can only be used as the single card he selected; the details of that card are shown and the magnetic stripe is activated, but no other interactions with the device are possible. He hands the Card3000 to the teller who swipes it through the reader on the register and hands it back to Kevin. He then locks the card so that it cannot be used for any further transactions, even if it's stolen. Now Kevin can stop carrying so much cash, and start earning reward points, all with the peace of mind of knowing that Card3000 is keeping his personal data secure.

Following a purchase, Kevin likes to review his recent transactions to ensure that the correct amount was billed. After paying for a $3.99 coffee with his Card3000, Kevin swipes up in the interface to see the last 5 transactions on the card. He sees the $3.99 coffee purchase, which looks fine, but then he also something odd: a $62 transaction at a gas station. Knowing that he never uses this card for gas, and that his car can't even hold that much gas anyway, he realizes that this was a fraudulent transaction. He taps on the line item, and selects the "report fraud" option. The Card3000 notifies the credit company, and asks Kevin if he wants to freeze the card. He chooses "yes", and that card number is immediately inactivated, protecting him from any more attempted theft.