Phase 1 Documentation

Isabella Tromba, Isra Shabir, Kevin White

Primary Author here onward: Kevin

Motivation

For most group purchases, one person is normally responsible for paying the bill and being reimbursed later for efficiency. There should be a way to detail how much each party owes and for that party to pay it without having to go through the process of wiring, paying in person, or even having to run after parties for payment.

Purpose

Splitting costs for a joint purchase and reimbursing the person who has paid a group tab**.**

Goals

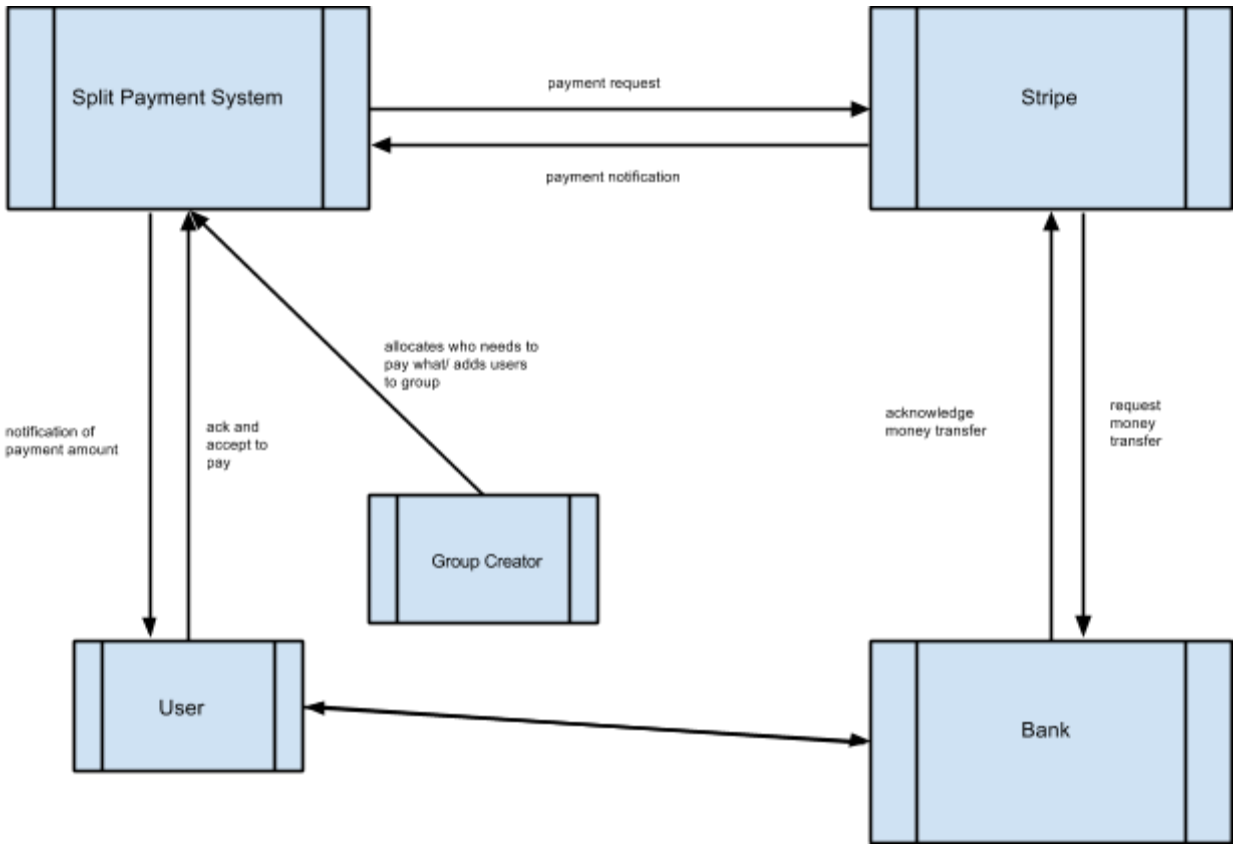
- Easily document the breakdown of payments for a group purchase
- Provide a method of secure online payment
- Allow communication between members of a group purchase to allow for fast and efficient splitting of costs.

Key Concepts

- Group- Group is a representation of a all the people who participated in a given purchase
- Creditor (the member who's made all the payments) - Also known as the group creator, this will be the recipient of all payments in the application as it is assumed he/she paid for the actual purchase
- Invoice- A message on the group page detailing money owed by a party to the creditor with an explanation as to why

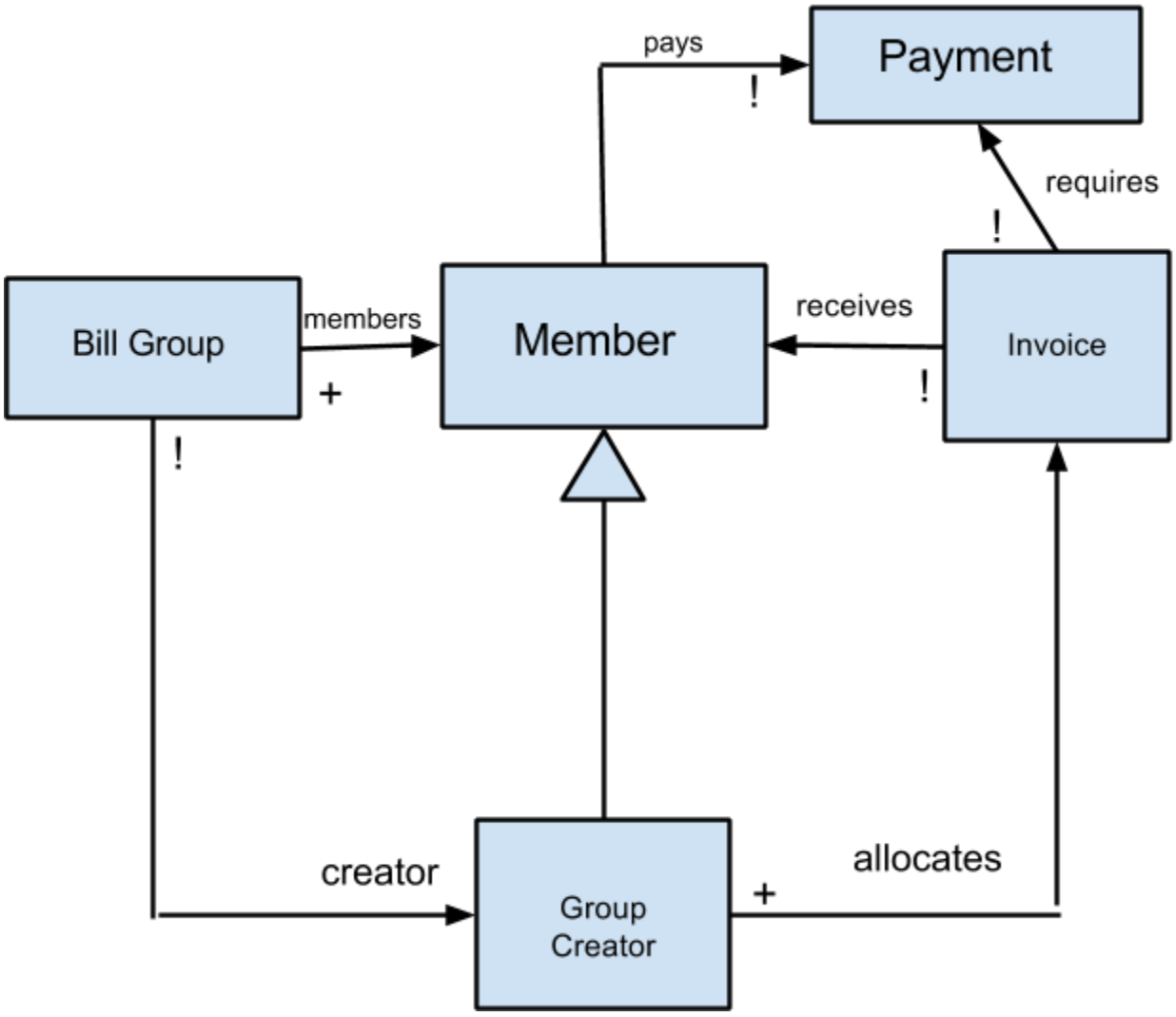
Primary Author here onward: Isabella Tromba

Context Diagram



Data Model

A group creator creates a bill group and invites members to join this group. The group creator is responsible for allocating invoices to each of the members. Each Member of the group receives an invoice and pays the amount specified on the invoice. The invoice requires a payment



Primary Author here onward: Isra Shabir and Isabella Tromba

Feature Descriptions

Group Creator: One user creates the group that needs to split a payment - this user can choose whether to split the amounts paid evenly or to manually allocate who pays what. They invite the other users to the group bill.
Team communication: Members of a group can post comments and communicate to resolve any conflicts (or just use it as another secluded talking medium!)
Payment Dues Visibility: Each user will be able to see who the admin of the group is and the amount they and all others have to pay.
Safe Payment System: Once the payments are allocated, users will use STRIPE and enter their credit card information to make a payment.

Security Concerns

Security Requirement: Adhere to PCI guidelines when taking credit card info/dealing with e-commerce on website
Addressed: Being PCI compliant is very costly so doing this for our app is not going to be feasible. Instead, we will use a third party payment system (Stripe) that through cross-domain AJAX is able to send credit card info directly to their server. We will not be responsible for storing users' credit card information. Stripe is a well established third party API for such transactions.

Security Requirement: Secure data transfer. All user information (password/address/etc) must be protected.
Addressed: Data will always travel on secure channel: https. All password data will be encrypted and authenticated according to IPsec (Internet Protocol Security)

Security Requirement: Secure storage of data on the server.
Addressed: All data stored on the server (user passwords/ user information) will be encrypted.

Security Requirement: Payments that are made are valid and come from valid credit card numbers/ real people
Addressed: User Stripe for credit card validation and to track successful payments.

Security Requirement: User Access Control.
Addressed: Only users who have permissions(must be authenticated and authorized) to view a groups bills can do so.

Assumptions about attackers

Outside Attacker:

- They are interested in credit card information
- They will not be one of us .
- Attackers can use packet sniffers to capture data as it is sent over the internet

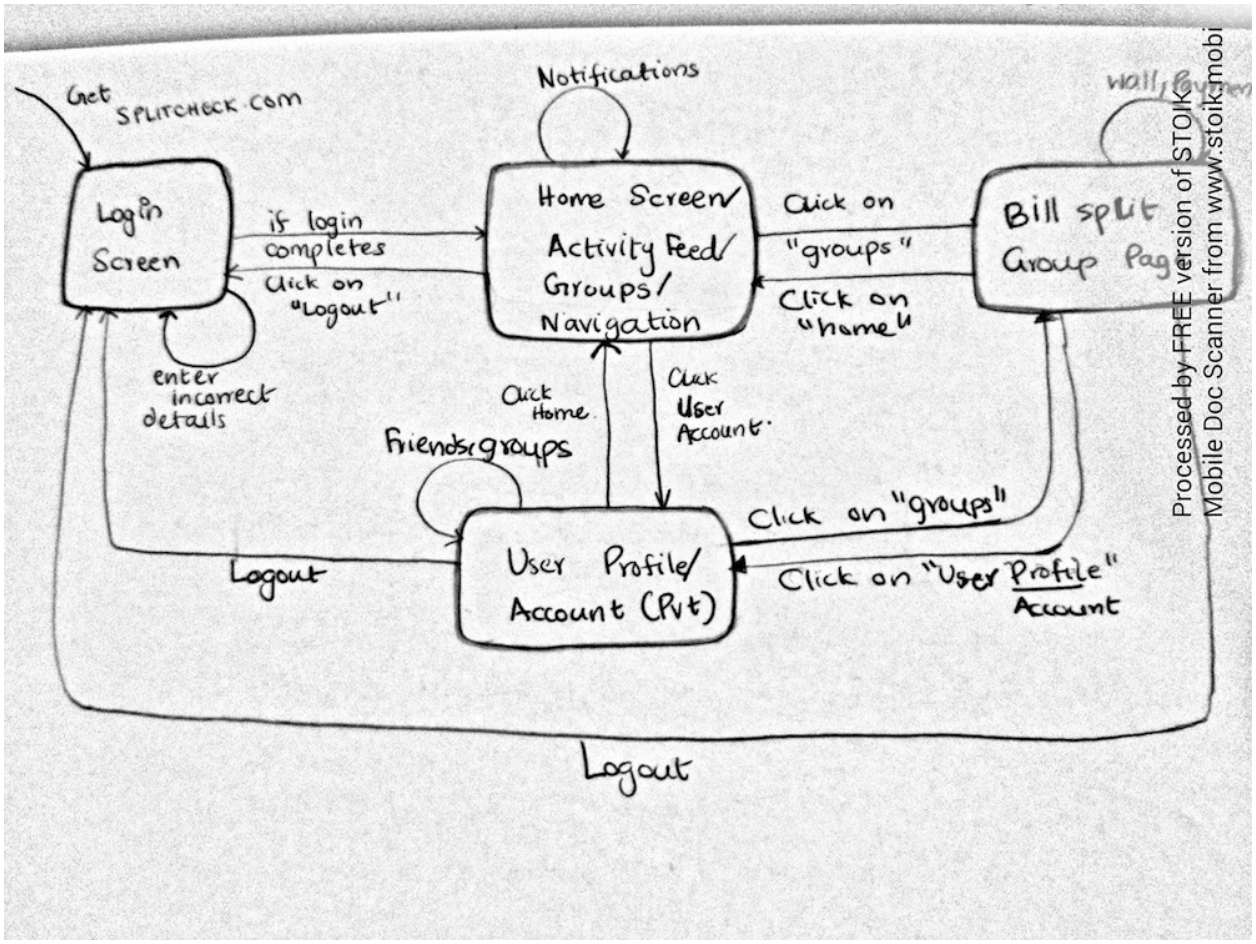
Current User:

- Denial of Service Attacks
- Could be a user who is interested in generating a fake payment.

Primary Author: Isra Shabir

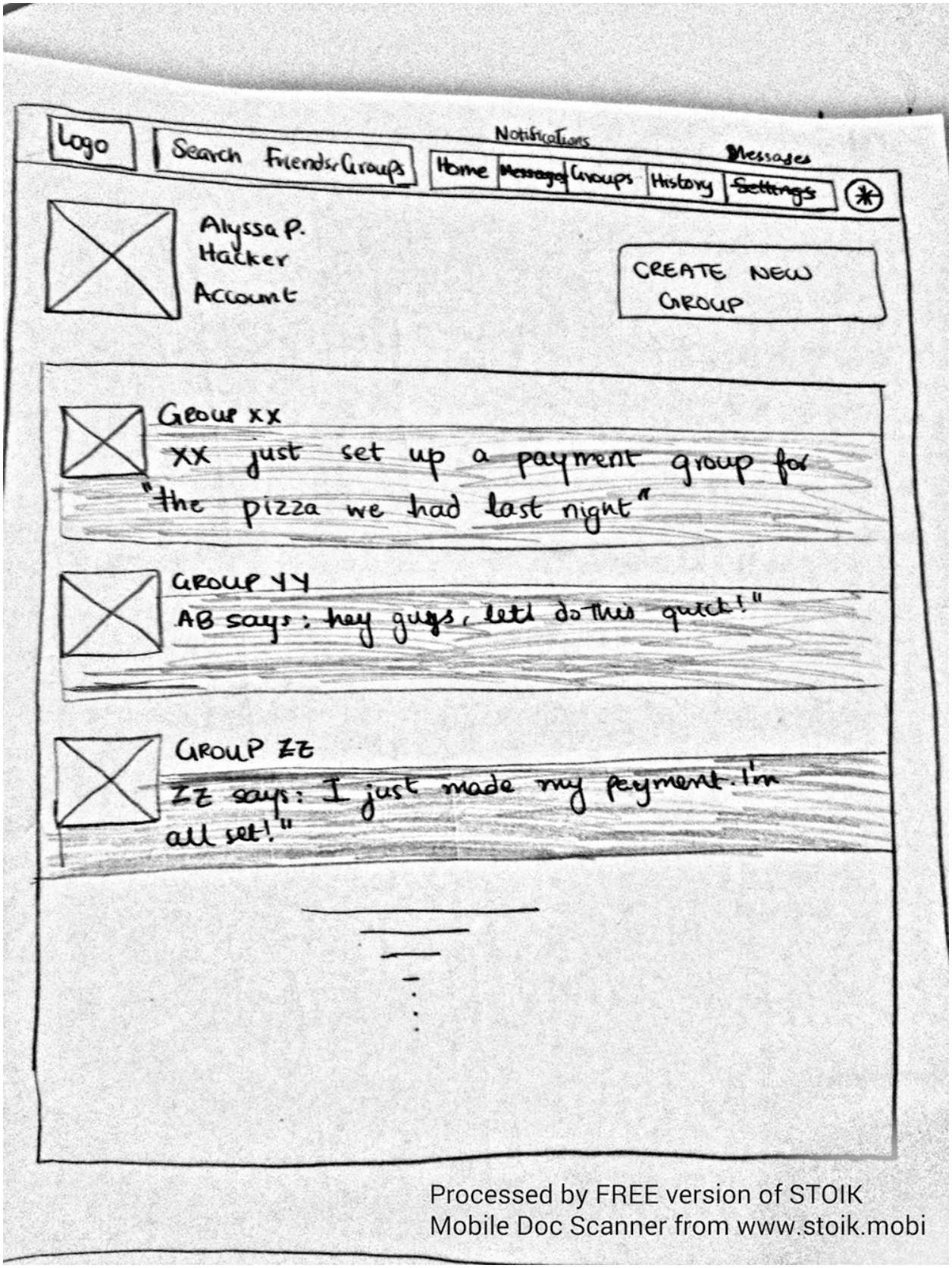
User Interface

The Flow Chart and the Wireframed page layouts are on the pages to follow.
Error handling for events like incorrect passwords is done in such a way that the user will be re-directed to the same page until correct credentials are provided. User Account is lockeda after 5 unsuccessful attempts. Same thing happens when users try to enter incorrect Credit Card info (this, however, will be handled by the 3rd Party API - Stripe)

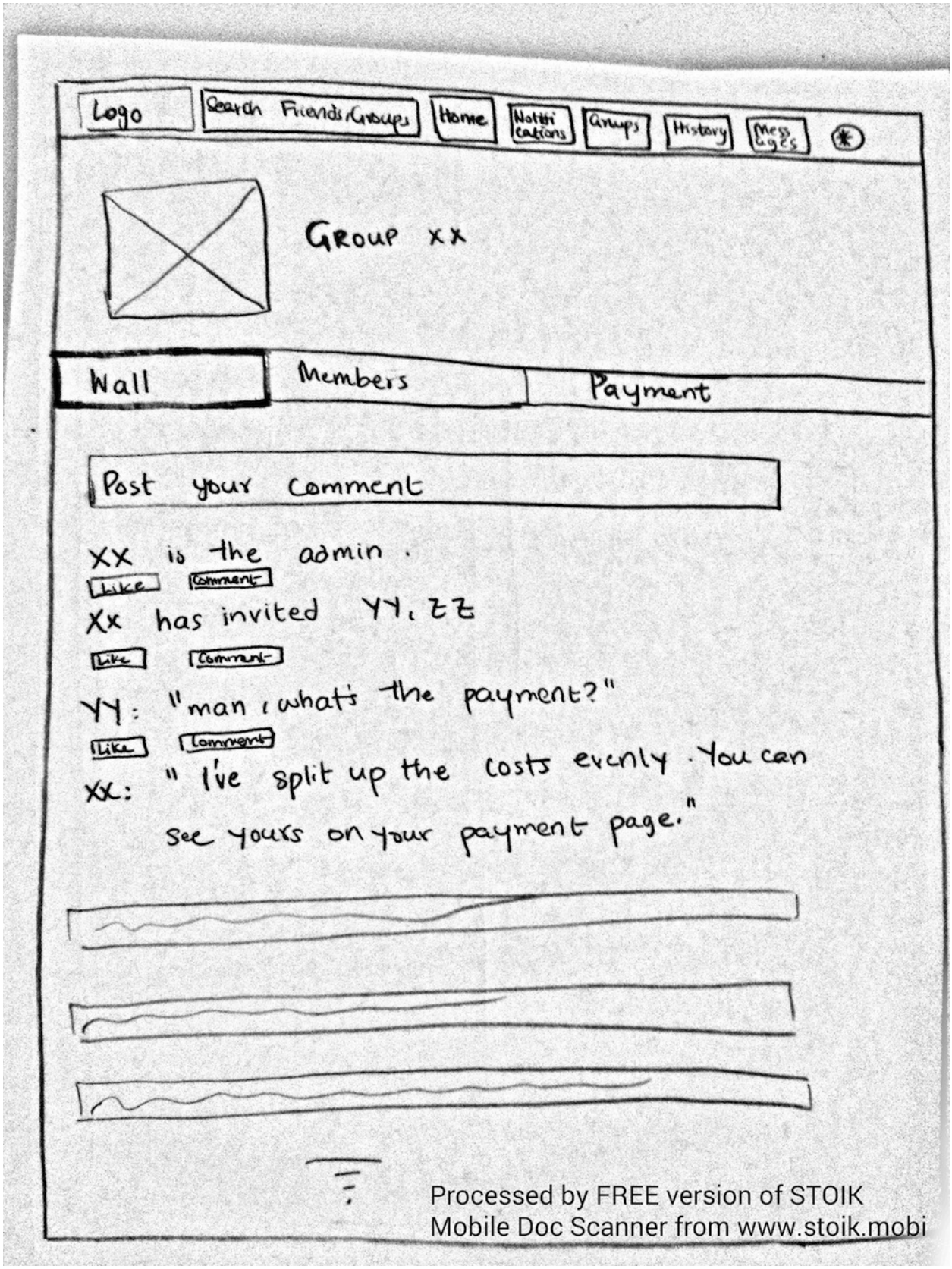


Flow Chart for State Machines with transitions.

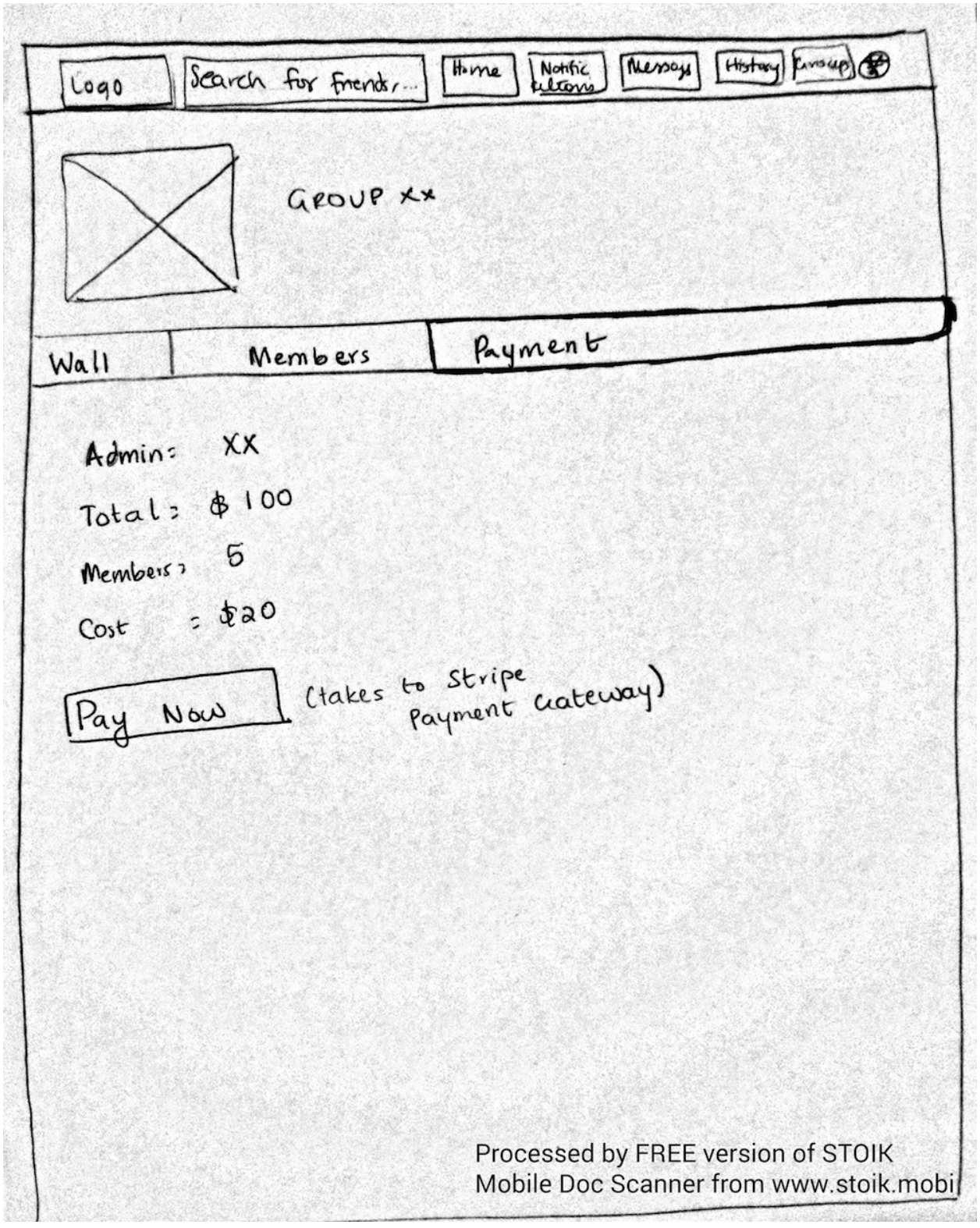
WIREFRAME - Page Layout 1



Upon clicking “Groups” on the Activity Feed or on the navigation bar above: Page Layout - 2



Layout Page 3 - Payment tab under Groups



Layout Page - 4. User Account (private)