# **Product Improvement**

**Table of Contents**

[**Product Improvment** 1](#_Toc127496116)

[**1.1 Monay Wallet** 1](#_Toc127496117)

[**1.2 Monay Portal** 10](#_Toc127496118)

[**1.3 Admin Portal** 13](#_Toc127496119)

## **1.1 Monay Wallet**

**1. Auto top-up**

* 1. User will agree to auto-top-up terms and conditions
  2. Monay wallet will recharge the wallet if it goes below a specific amount
  3. The amount on which auto top-up will occur shall be decided by the user
  4. Only primary users can use an auto top-up feature
  5. Bank details will be saved
  6. Users don’t need to take any action
  7. No 2FA will be required on auto top up
  8. Only cards that won't ask CVV on recharge will be applicable
  9. ACH option in auto-top-up will be provided

**2. Minimum wallet balance & refill amount.**

* 1. After a minimum amount user will be notified to recharge the balance in the Monay wallet

**3. Limit multiple secondary accounts**

* 1. The primary user can restrict the amount for the secondary user

**4. Enable/Disable secondary user by primary user**

* 1. The secondary user will be by default disabled, primary user will enable to activate the secondary account
  2. **Sharing the Monay App Primary account:**  The Monay app allows registering other family members or work/office members under the primary account. The Monay App uses Primary and Secondary user features that links the users together for using the App and providing necessary co-user approvals and authorize their access.

**5. Primary user as a secondary user of another primary user.**

* 1. At a time, the user can either be a primary or a secondary user**.**
  2. The secondary user can choose a relation with the primary user
  3. Maintain a relationship between primary and secondary accounts.
  4. While the secondary user is registering secondary user will be allowed to use the primary user and relation (dropdown) with the secondary user.
  5. The same phone number and email can be associated with multiple accounts: primary and secondary
  6. The user will be identified by phone number and a flag: primary or a secondary use

**6. QR code to be used for referrals.**

* 1. QR code will be for registration and payment

**7. Biometric Information**

* 1. Users can login to the Monay wallet application with their fingerprint and Face ID.

**8. Buying Products**

* 1. Users can avail features such as buying groceries ,clothing to purchasing insurance and stocks.

**9. Ready Cash**

* 1. Monay provides small terms and instant digital loans to the users
  2. Certain limits of the loan will be decided according to the user's cash flow using Monay wallet.
  3. Users can avail ReadyCash service for a duration of four weeks; with the option to pay back early as well.
  4. A user can get only a single loan at a time of up to INR 10,000.
  5. The eligibility criteria of Ready Cash is that the user should have a cashflow history of 10,000 INR.

**10.** **Stock and crypto trading.**

* 1. Users can trade stocks and cryptocurrency using the Monay wallet

**11. Payment on third-party applications**

* 1. Monay wallet API should allow payments on third-party applications like food delivery, taxi-hailing, restaurant, hotel booking, and gaming.

**12. Charity donation feature**

* 1. Monay wallet can be integrated with reliable charity organizations in the country, where users can donate

**13. A bill management tool**

* 1. Monay wallet can help users track, review, and pay their bills.
  2. Reminder notification before due date if the bill is unpa

**14. Gift card and reward offerings**

* 1. Monay wallet allows users to create a gift card for the users. A promo code will be generated by the system which can be used on the e-commerce website.
  2. On using of Monay wallet features, users will be offered loyalty rewards
  3. Partnered with all major shopping carts and eCommerce platform to provide reward offers using Monay wallet

**15. In-store QR Payments**

* 1. In-store QR Payments can be made using the Monay wallet

**16. AI-powered financial assistants**

* 1. Monay wallet help users make smart, customized decisions about their money.
  2. Budgeting features using AI can give analysis or insight according to customers' data
  3. Smart financial assistants such as smart advisor who continuously reviews clients’ subscriptions and bills, manages their budgets, proposes saving and investing strategies, and provides other relevant feedback on how to reach financial goals.
  4. Smart assistants can notify users of discounts at their most frequented stores while shielding them from incessant marketing, creating custom budgets, or seeking out the best loan rates and insurance options based on a specific user’s needs.
  5. Remind users to pay their bills
  6. AI-based chatbot provides message-based personalized advice to users and answers questions on whether they can afford something

**17. Implement Adhar pay (For India)**

* 1. Adhar Pay is the most common digital platform used in India. Even small consumers particularly farmers are using it frequently due to its ease of use.  Integrate Adhar Pay with Money wallet to increase the reach of the wallet services.

**18. KYC Verification (For India)**

* 1. To make the registration process user. KYC process should have minimum fields. Verification of the KYC process can be done by Adhar's number.
  + Adhar number
  + Real-time picture capture
  + Pan card number
  + Bank Account number

**19. Geo-Coded Push Notification App**

Fetching the location of the user by Monay Wallet application, Geo-Codes can be set for Toll Roads / Toll Plazas, Parking lots, violation fee, EV charging slots, and Location-based Push Notification Campaigns Push notifications can be sent on the app using Nudge.

**Push Notifications**

1. Toll Ahead Exists Now
2. Toll Ahead
3. Toll Started
4. Exiting Toll – Pay Now
5. Toll Ahead – Fund Wallet Now (your balance is zero)
6. EV charging availability
7. Book a parking reservation

Monay App can be integrated with Android Auto and Apple CarPlay App for better geo-coded features. The following features can be useful for the Geo Coded feature in Monay Wallet.

**Android Auto**

Real-time alerts with Google Maps, Waze, and other navigational apps. Google Assistant can find gas along the way, check EV charging availability, or book a parking reservation for when you arrive. A car’s dashboard display helps to know more about what’s nearby.

1. Find routes
2. Real-time alerts
3. Places on the way
4. Reserve parking

**Apple CarPlay**

CarPlay supports third-party navigation apps directly from the Dashboard.

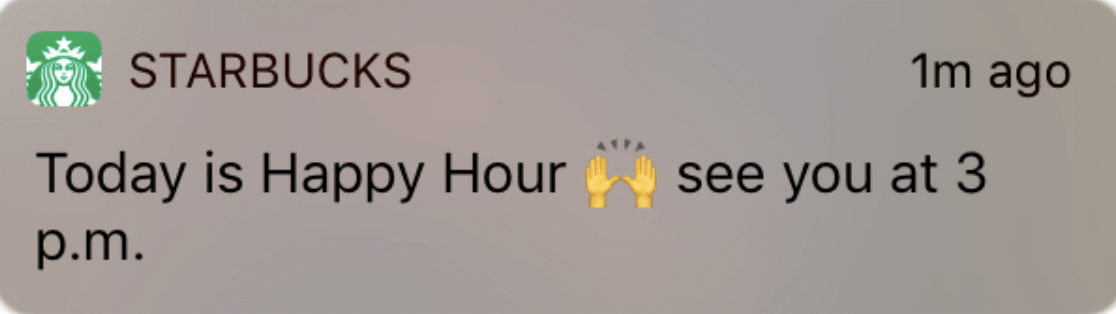
* 2GIS

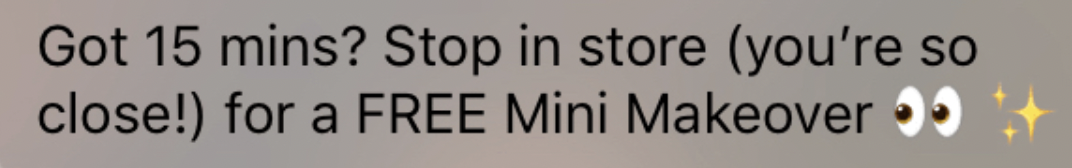
1. Autonavi Map
2. Baidu Map
3. Google Maps
4. KakaoNavi
5. NAVER Map
6. NAVITIME
7. Sogou Map
8. Sygic Car Navigation
9. GPS & Maps
10. Tencent Map
11. T Map
12. TomTom
13. Waze

**Location-based Push Notification Campaigns**

Monay wallet API should allow payments on third-party applications like food delivery, taxi-hailing, restaurant, hotel booking, and gaming.

* The brand campaign uses the customer’s general location data and time zone to create a prompt that feels personalized, drives users to a nearby store, and encourages them to use the Monay wallet to pay for the order. The promo invites app users to come to their nearest Starbucks shop to participate in a buy one, get one free “Happy Hour.” First users receive the invite push notification. When they open the message, they’re brought to a screen in the Monay app that explains the promotion, then directs them to find their nearest location.



* For ordering app, reminds users to make their order by suggesting local restaurants, and gaming spots they may want to eat at, and offering them a $5 discount if they pay by Monay wallet. Suggesting a local store or location users love in your promo adds a layer of personalization. Another important factor is the timing of this push notification. This one is sent before noon—the time users typically start thinking about making a lunch order on the app.
* Personalized notifications about events, sport match according to location and prefer to pay through Monay app.
* Class or event passes: If a customer uses an app to purchase a class or attends a nearby event, send them a push notification for other top-rated classes or similar events in the area.
* Weather-based promos: Brands could send location-based messages to customers in certain regions about seasonal promotions based on local weather forecasts. Ex: “It’s going to be chilly in Cleveland this week. Stock up on winter gear with the coupon code CHILL20 at your local store.
* promotions are geo-triggered when a mobile user is within the boundaries of a pop-up shop, retail store, or other special event or location.
* Travel-based promos: Telecommunications companies often send customers messages about buying top-ups when they travel. Think about how your brand can show users value when they leave their city or country by sending them special offers, helpful information and more. Ex: “Welcome to Orlando! Forget to pack something? Stock up at our downtown location at 321 Sunnyvale.”
* Engage users when they leave a location: Consider sending a push notification after users leave a geofence. Offer a discount the next time they’re in the area, or ask them for a review of their experience (if they made a purchase or entered your location) to stay top of mind and gain valuable feedback.
* Live-event offers: Sponsors of a live event, like a concert or sporting event, could send push notifications to mobile users near or at the event to visit their booth for a special promotion.

**20. Wallet**

supporting all current types of wallets (both google and apple). The editor will need to support wallet design and link it to the Emails and SMS nudges as merged Tags. Preconfigure Templates for Wallets can be provided that can be editable at predefined places/locations on the Wallet Pass

**21. Online Bank**

**22. Vehicle**

User can add and manage vehicle information to Monay wallet. Licence plate number, State of registration is required to add a vehicle. Option to scan Licence plate can be integrated to fetch vehicles information. One user can add multiple vehicles to the application. Each vehicle, location tracking should be enabled. Integration with GPS tracking unit is required for vehicles location tracking.

1. **Toll**
   1. **Subscription**

The user would be asked to download the tolling app Monay powered by Worldpay. The Monay App needs to be marketed by the tolling agencies involved in this RFI. We will make QR codes available for promoting the download of the app at toll booths, toll plazas, online as well as in newspaper, or travel magazines.

* **Registration**

The user would be asked to register their automobiles in the app as a starting point, by adding their license plates. The app would check against the state databases to confirm the license and class of automobile / vehicle for enabling the correct toll-pricing and billing.

* + **Mobile Wallet**

The Monay app would allow loading money into the wallet for paying the toll, with an auto-replenishment feature when a certain minimum threshold is reached. This enables pre-paid feature for toll users as well as the ability to top it up at a toll plaza with cash if needed. The wallet allows for splitting toll fares or pay other drivers for tolls for the use of their vehicle or specific tolls for a designated period. Merchant users can benefit from the top-up process as an incentive to participate in the eco-system.

* + **Paying Toll Scenarios**:
* ***At a toll gate***:

*Unregistered users - manual approach*: The occupant scans a QR code at the toll gate and pay for the toll. As an option, a set of cameras at the toll gate takes a front/back picture of their license and sends the images to the occupant, requesting validation of the contact details and to confirm and register the vehicle in the Monay App with the tolling agencies.

QR codes on the toll plaza, Worldpay Payment Gateways, Tilli.CX tech stack, Nudge.PRO notifications, and Monay wallet App. The solution will allow the Toll Agencies to provide a dynamic QR Code for placing it at the Toll Plaza at current state facilitated by Worldpay from FIS.

The solution leverages existing infrastructure in place i.e., users’ Smart mobile phones with GPS, alternative navigation tools, smart watches, public cellular network, and cameras. Worldpay from FIS can provide a pilot in a specific region / toll location in partnership with any of the Participating Toll Agencies for testing the Nudge.PRO / SmartPay solution and rolling this out.

*Unregistered users* - automatic approach: A set of cameras at the toll gate takes a front/back picture of license, the images are sent to the back office in real-time, and the back office system converts the license images to alphanumeric values and looks up the automobile registration database and sends the auto-owner registered with DMV a Nudge (text and/or email message) with the images of license for them to confirm and validate the contact details and pay the toll using our SmartPay page. This is a post toll feature (postpaid).

*Registered users*: When a user wants to use a toll, they simply open Monay app, and the app automatically connects to the network and based on the GPS location of the mobile device, auto-calculates the necessary toll by the back-office systems using the current GPS segments (Geo-codes) as per the Monay App present in the vehicle. Also, a “No toll-due at this location” would be shared for roads that do not have a toll. This is also a post toll model, however the wallet would need to be prepaid /prefunded for enabling auto billing post toll.

* ***On a toll road***:

*Unregistered users*: A set of existing cameras at the toll road start and at the exist, take a front/back picture of license, the images are sent to the back office in real-time, and the back office system converts the license images to alphanumeric values and looks up the automobile registration database and sends the registered vehicle-owner a Nudge (text and/or email message) with the images of license for them to confirm and validate the contact details and pay the toll using our SmartPay page. This is a post toll feature (postpaid).

*Registered users (Auto Toll Billing)*: The Monay app will track the start and end of the ride and auto-bill the user for the toll-usage. The Monay app will need to be running to do this enroute. Based on the segmentation as configured in the back-office system, the app user would be billed based on the toll usage against the type of the automotive registered with the Monay App. The back-office integration is needed only for real-time billing based on usage of toll and current price for that toll segment considering the vehicle classification.

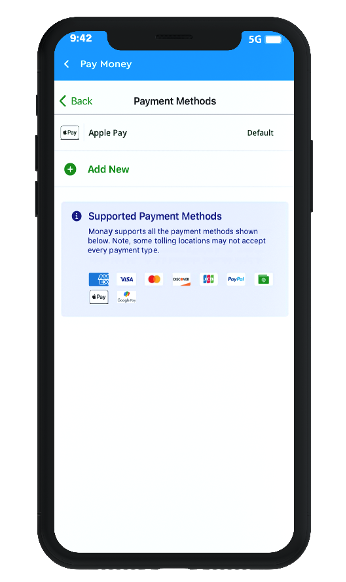
The Monay App will integrate with Nudge to provide the current geolocation for triggering the personalized push notifications relevant for that toll location. Geolocation push notifications are **automated push notifications that get triggered based on Monay subscriber's location**. Geolocation notifications are great for promotions, informational updates, and transactional notifications alike.

This would allow bypassing any markers (toll plazas). This is also a post toll model, however the wallet would need to be prepaid /prefunded for enabling auto billing post toll.

Auto-bill: If we think about the ride share model, payment isn’t processed until after the trip is completed and the costs are already calculated in advance of the ride. We can calculate the tolls for the driver, who then completes the journey without by passing any markers (toll plazas).

Payment Methods: ApplePay, GooglePay, Visa, Master Card, Discover, Amex, Cash, Paypal, Crypto currency (e.g., Bit coin) and Cash (pre-paid)

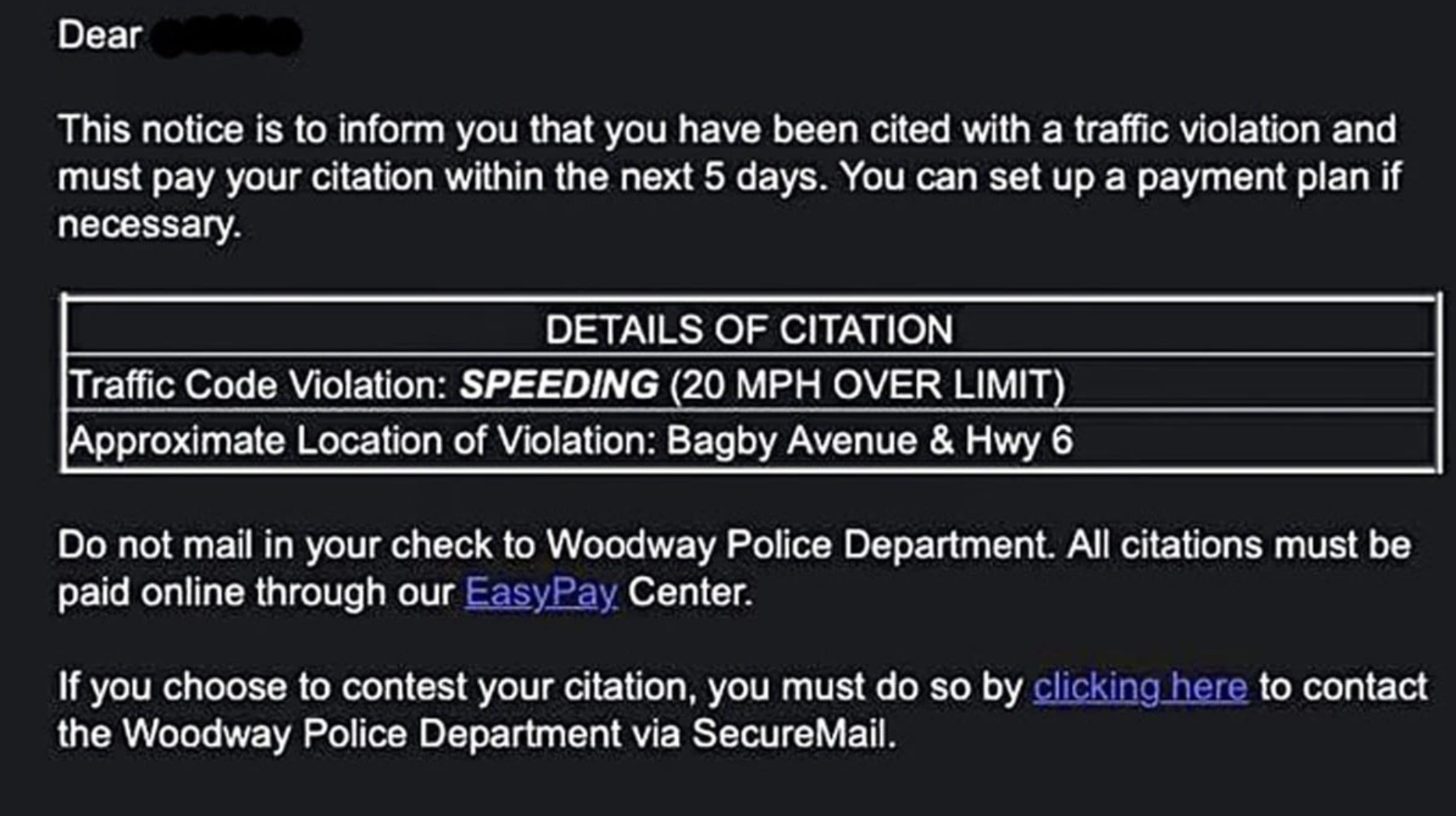
QR codes on the toll plaza, Worldpay Payment Gateways, Tilli.CX tech stack, Nudge.PRO notifications, and Monay wallet App. The solution will allow the Toll Agencies to provide a dynamic QR Code for placing it at the Toll Plaza at current state facilitated by Worldpay from FIS.



The solution leverages existing infrastructure in place i.e., users’ Smart mobile phones with GPS, alternative navigation tools, smart watches, public cellular network, and cameras. Worldpay from FIS can provide a pilot in a specific region / toll location in partnership with any of the Participating Toll Agencies for testing the Nudge.PRO / SmartPay solution and rolling this out.

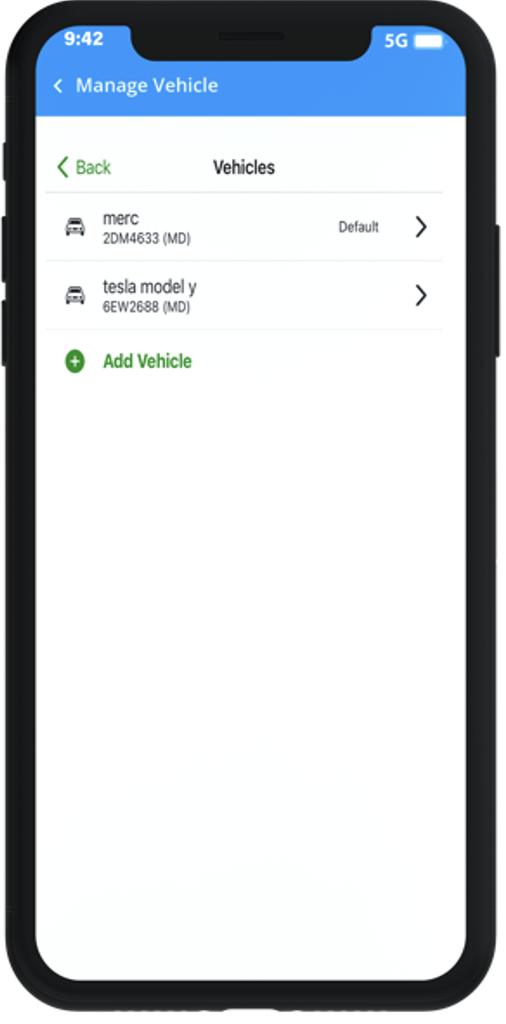
* **Prepaid toll fee** can also be paid from Monay wallet

1. **Violations** 
   1. Payment of e-challans
   2. Violation fee: Users can track and pay violation fee



1. **Parking fee**
2. **Location**

For the main pages: -> Vehicles -> Manage Vehicles.



For Add Vehicle:

Note – for these vehicles, we will need to enable location tracking.

**Target By Latitude and Longitude**

The solution would allow toll authorized representatives to view, edit and enabling segments of a map (collection of geo-codes) representing the toll lanes by the authorities that manage tolls and toll roads, which identify the billable segments on a route. If a GPS enabled smart mobile device was found to be traveling on that segment, and if the app was installed and enabled, the app would bill the owner for the segment of the toll based on existing pricing imposed by the tolling authority at that given time based on the classification of the vehicle such as “Class: 2 axles, 4 tires (up to 7,000 lbs) = IAG Class 72”, etc.

<https://developer.apple.com/documentation/corelocation/creating_a_location_push_service_extension>

<https://developer.apple.com/documentation/corelocation/cllocationmanagerdelegate/1423615-locationmanager>

If your Mobile App collects location data, OneSignal will automatically update the latitude and longitude for the device based on the location permission granted by user.

* For iOS location settings, see the [Apple Developer Guide for Choosing the Location Authorization Level](https://developer.apple.com/documentation/corelocation/choosing_the_authorization_level_for_location_services). Apple requires a description be set in the project's Info.plist to display the authorization dialog. Set either the [NSLocationWhenInUseUsageDescription](https://developer.apple.com/documentation/bundleresources/information_property_list/nslocationwheninuseusagedescription) for requesting authorization only while app is in focus or [NSLocationAlwaysUsageDescription](https://developer.apple.com/documentation/bundleresources/information_property_list/nslocationalwaysusagedescription)for usage at all times.
* For Android location settings, see the [Android Developer Guide on Location Permissions](https://developer.android.com/training/location/permissions).

You can ask for location tracking permission through our [Location Opt-In Prompt](https://documentation.onesignal.com/docs/location-opt-in-prompt)

The system will work as described below:

* **Subscription**:

The user would be asked to download the tolling app Monay powered by Worldpay. The Monay App needs to be marketed by the tolling agencies involved in this RFI. We will make QR codes available for promoting the download of the app at toll booths, toll plazas, online as well as in newspaper, or travel magazines.

* **Registration**:

The user would be asked to register their automobiles in the app as a starting point, by adding their license plates. The app would check against the state databases to confirm the license and class of automobile / vehicle for enabling the correct toll-pricing and billing.

* **Sharing the Monay App Primary account**:

The Monay app allows registering other family members or work/office members under the primary account. The Monay App uses Primary and Secondary user features that links the users together for using the App and providing necessary co-user approvals and authorize their access.

4: **Mobile Wallet**:

The Monay app would allow loading money into the wallet for paying the toll, with an auto-replenishment feature when a certain minimum threshold is reached. This enables pre-paid feature for toll users as well as the ability to top it up at a toll plaza with cash if needed. The wallet allows for splitting toll fares or pay other drivers for tolls for the use of their vehicle or specific tolls for a designated period. Merchant users can benefit from the top-up process as an incentive to participate in the eco-system.

**23. Transit**

Railway, airplane tickets fares can be paid through wallet.

**24. Payment of tax**

**25. Multicurrency account**  
Access and manage multiple currencies. Improve conversion rates.

**26. Planned Payments**

Recurring payments can be planned which will automatically pay on a specific interval. A reminder can be sent 24 hours prior to sub-merchant before the payment is paid.

* Utility bills can be set before due date
* Sub-merchant can manually stop the payment anytime from the application
* An option to disable the payment can be integrated in reminder email.
* Account to be transferred, date of transfer, amount can be specified or automatically fetched from the bill reference number.

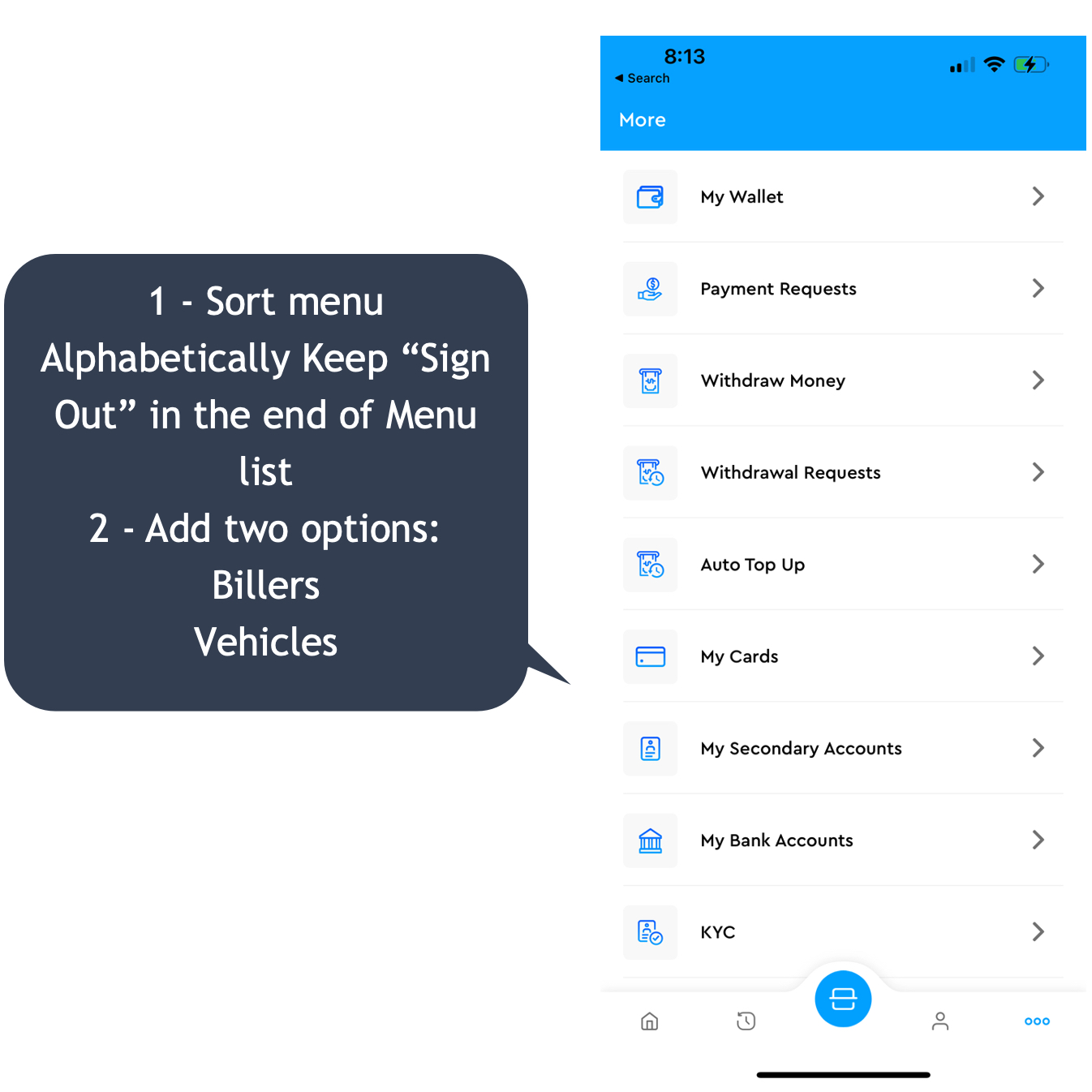
Graphical user interface, application

Description automatically generated

**27. Changes to the Menu**

1 - Sort menu Alphabetically Keep “Logout” in the end of Menu list

2 - Add two options: Billers & Vehicles



## **1.2 Monay Portal**

**1. Payment links**

* Payment links are supported in international currency
* Set reminders for Payment Links: An automated SMS and email reminder for the Payment Links can be set. It will help increase the number of paid Payment Links, Reduce the cost and manual effort required to collect payments, and reduce the number of days taken by the customer to make the payment.
* **Create Contacts :** Contacts can be created for recurring customers. Instead of creating and processing payment links one by one, bulk upload feature can be integrated to process payment links in bulk.

**2. Refunds**

Improve refund, void and chargebacks to be processed immediately to improve customer experience, increase product value and increase sales.

**3. Integration of sub merchants account statement with accounting software**

Integration of sub merchants account statement with accounting software to sync payment information and reconcile payments statements. The transaction data on the payments statement flows into accounting software, saving the time and effort.

* Sync can be scheduled at a fix time by sub merchant or automatically occur after every 8 hours.
* Integration with famous accounting software's like Zoho CRM, Zero and QuickBooks can be setup.

**4. Dashboard**

* Include Support Tickets Inbox option on Dashboard. To raise queries in case of trouble and follow up on the existing ones.
* Include Documentation and FAQs navigation.

**5. Settings**

1. **Change checkout theme:** The theme colour of the portal’s web pages can be changed.
2. **Select language:** The user can view the content on the web page in their preferred [language. By](http://language.by/) default language is English.
3. **Enable international payments:** The sub-merchant can accept payments in various international currencies supported by the Monay GPS. If the sub-merchant does not want to accept payments in currencies apart from USD, the user can turn it off using the toggle switch.
4. **Payment methods:** A list of payment methods and their status will be displayed. Payment methods such as Mastercard, VISA card, Bitcoins e-cheque, and wallet.

**6. Scam Transaction detection**

Payment gateway is a powerful fraud prevent tool. When configured properly, it can halt fraudsters in their tracks and save your reputation.

* **Address Verification Service (AVS)**  
  AVS is an effective security measure to detect online fraud. When customers purchase items, they need to provide their billing address and ZIP code. An AVS will check if this address matches with what the card issuing bank has on file. Part of a card-not-present (CNP) transaction, the payment gateway can send a request for user verification to the issuing bank.  
  The AVS responds with a code that will help the merchant understand if the transaction has a full AVS match. If they don’t match, more investigation should be carried out by checking the CVV (Card Verification Value), email address, IP address on the transaction or allow your payment gateway to decline the transaction.
* **Declined Transactions**

To detect fraud in declined transactions GPS should automatically send customer an email asking for an identity confirmation, new card or new payment method. Decline codes from the gateway should also be tracked.

* **Chargebacks**

Requested chargebacks should be monitored.

* **Fraud Analysis Dashboard**

Use all the data of transactions to make intelligent, tailored fraud decisions. A dashboard that gives deep and actionable insights into how fraud impacts the business. Optimize the user experience and payment flow, while keeping it secure. Strategies to adjust risk thresholds, adapt new threats, reduce chargebacks and accept more business should be implemented. Make rapid decisions based on enhanced data analytics and fine-grained profiling .Gain a single customer view with solutions spanning portfolios, products and brands

**7. Scam Transaction prevention**

* **Card Verification Value (CVV)**  
  The CVV (or Card Verification Code) is the 3 or 4-digit code that is on every credit card. The code should never be stored on the merchant’s database. A CVV filter acts as an added security measure, allowing only the cardholder to use the card since it is available only on the printed card. If an order is placed on your website and the CVV does not match, you should allow your payment gateway to decline the transaction. While making a card-not-present transaction (online, email, or telephone orders), the merchant gets the required card information from the customer to verify the transaction. Friendly fraud is a risk associated with CNP transactions that can lead to a chargeback. Enabling a CVV filter helps sight fraud and reduce chargebacks.
* **Risk scoring**

Risk scoring tools are based on statistical models designed to recognize fraudulent transactions based on several rules. When a payment is done on the website, the tools will indicate the probability of the transaction being fraudulent. A higher probability of a transaction being fraudulent indicates that you should verify the order.Risk scoring tools provide a case by case evaluation and will flag transactions based on the rules you choose such as AVS failure test, IP range, use of anonymous emails, billing address and others.

* **Device Identification**  
  Device identification analysis of the computer rather than the person who is visiting your website. It profiles the operating system, internet connection, and browser to gauge if the online transaction be approved, flagged or declined. All devices (phones, computers, tablets, etc) have a unique device fingerprint, similar to the fingerprints of people, that helps identify fraudulent patterns and assess risk if any.  
  Companies like ThreatMatrix, monitor the device ID, using it as a reference point to see if other people have flagged it as be approved for suspicious or fraudulent activity. Fraudsters cannot impersonate a computer’s unique identity, making it a viable option for protecting your business against online fraud.
* **Flag Large Transactions**  
  With stolen card information, fraudsters will take a shot at making large transactions before the card is blocked. This would be deleterious to your business (big or small) where you will have to bear the cost of allowing a fraudulent transaction to take place. It can also lead to a payment processor terminating your processing account, and your business would take a big hit. You can limit the number of large transactions by specifying a flat transaction amount, which is an essential step towards avoiding chargebacks. In addition to this, you can limit the number of failed transactions that go through the payment gateway.
* **Payer Authentication (3-D Secure)**  
  Payer authentication, also called Verified by Visa (VeB) and MasterCard SecureCode, is a cardholder authentication measure that secures online transactions for customers. This method allows cardholders to create a PIN (secure code) that can be used during checkout to confirm the user’s identity. By implementing this, merchants are provided chargeback protection and lower interchange rates.  
  This is one of the most sought-after fraud prevention tools that businesses undertake that also looks after their interests.
* **High-Risk Countries**  
  For international transactions an extra layer of security should be kept for high-risk countries. Customers in these countries have to call the company to verify their identities before their transactions are processed. According to the Online Fraud Guide, some of the countries with the highest online fraud rates are Israel, Malaysia, Egypt, Pakistan, Ukraine, Russia, Bulgaria, Romania, Lithuania, Nigeria and Yugoslavia.
* **Lockout Mechanisms**

The lockout mechanism is a type of fraud prevention system meant to deter fraudsters who use automatic card number generator programs. These programs circulate in underground fraud forums and can generate hundreds of “valid” credit card numbers. The fraudster will typically try hundreds of numbers on your website until he finds some that are valid and will then charge the accounts to their limits.  
To prevent this fraud, merchants can:

* + Lockout transactions from a particular IP with many credit cards declined within a set time.
  + Disable transactions that fail the AVS test (since the fraudster will not have the account’s address).
  + When you detect such actions, you should immediately prevent orders from the originating address.
* **3DS**

3D Secure (3DS) is an important security protocol used by Visa and Mastercard (also known as Visa Secure or Mastercard Identity Check). It helps prevent fraud by allowing the issuing bank to verify that the cardholder is the same person making the purchase. Every time customer makes a purchase with the credit or debit card, the sub-merchant must ask the issuing bank whether the card is eligible for the transaction. The issuing bank will then authorize the transaction or decline it if it suspects fraud.

The 3DS process takes this one step further by adding an extra layer of authentication for both parties: the consumer and the sub merchant are given a “proof of ID” to complete the transaction in an added level of fraud protection. Consumers can verify their identity directly through their online banking account or via SMS verification, while merchants can use 3DS to generate a unique code that they can use in their anti-fraud system. This ensures that they know exactly who they’re dealing with and reduces their liability if something goes wrong with the payment. It is a 2 Factor Authentication (2FA) for transactions.

This process makes it more difficult for criminals to use stolen credit card details, because even if they have access to someone’s financial information, they won’t be able to perform the security check.

* **Transaction Limits**

Monay GPS should allow the sub-merchant to set transaction limits based on time of day, card number, and amount. Sub-merchant or admin can customize the limit depending on the scam transaction data of customers. Transaction limits can be set at a specific hour, on certain days, for holidays, specific weeks, and even months.

Sub-merchant or admin can also set a maximum number of transactions per card based on either the credit card number, the BIN (Bank Identification Number, or BIN code, refers to the initial sequence of four to six numbers that appears on a credit card) ,customer’s IP address and email. BIN is the most useful, based on our experience, because fraudsters like to bombard gateways with hundreds of attempts using the same BIN.

* **ReCAPTCHA**

ReCAPTCHA allows to block automated attempts to use stolen credit card numbers by requiring visitors to take an extra step to prove they’re human before submitting their information.

* **Void Transactions**

As a layer of security, system should automatically void transactions if the email or SMS of the receipt bounces. If correct contact information is not provided, there’s no way to reach out to the customer later and warn them of a fraud purchase or ask them to confirm the purchase was legitimate.

* **Fraud Scoring**

Fraud scoring tools use data to create a risk score for each transaction, which can be used to determine whether to accept or reject the transaction. Machine learning tools are used to analyze thousands of data points, including IP address, geo-location, device type and ID, email address age, proxy usage, payment history and more.

Fiserv Carat Fraud Mitigation evaluates every customer in milliseconds to provide a score and recommendation based on the assessment of the fraud signals of the

customer making the transaction. Every sub merchant is different

and so is the fraud, so Fiserv build fraud detection and machine-learning models around the business. The solution works to help reduce overall cost of fraud and increase revenue, by accepting more valid transactions, declining more fraudulent transactions and

minimize costly manual reviews.

**8. Explanation of KYC fields on portal**

Add a help symbol against each field in KYC and add a one liner explanation.

**9. Payment Reports**

The user should be able to download and email the report. Enter any email address or select owners added to share the report.

**10. Ticker symbol verification**

Real-time Ticker symbol verification.

**11. Detect fraudulent emails and prevent bogus email registration**

A third-party email address validator should be integrated to detect fraudulent [emails and prevent bogus email registration in real-time. It](http://emails.it/) should perform email fraud prevention analysis, Identify fake accounts, invalid user data, and high-risk behaviour for registrations, and payments. This helps maintain a clean and accurate email database of the sub-merchants. A tool powered by machine learning and AI that analyses hundreds of millions of email addresses per day across every region will be useful. Generate accurate email address reputation scores based on recent abusive behaviour, fraud reports, and signals from the user's activity, which measures behaviour across the web's most popular sites. Email address fraud scores are generated in real-time to identify risky accounts or payments. By validating email addresses in real-time it can ensure that we are only collecting real email addresses from business enterprises. This helps reduce CRM costs for unnecessary contacts and improve email marketing performance.

Email verification removes:

* **Disposable emails.**

This filter removes dummy and temporary email addresses.

* **Invalid emails.**

This removes any email address with an invalid format or that doesn’t link to an active inbox.

* **Misspelled emails.**

Catches invalid emails that were unintentionally submitted.

* **Spam trap emails.**

These are addresses that are specifically designed to catch spammers, since spammers rarely validate email addresses before sending blasts, and usually send emails without getting permission first.

* **Catch-all emails.**

This weeds out emails that start with “sales,” “support,” “admin,” and similar prefixes, so you don’t send emails to unmonitored inboxes.

* **Emails from new domains.**

Prevents fraud by eliminating emails that are hosted on brand new domains.

Email validation providers validate emails using a three-step process.

### Step 1: Syntax and Formatting

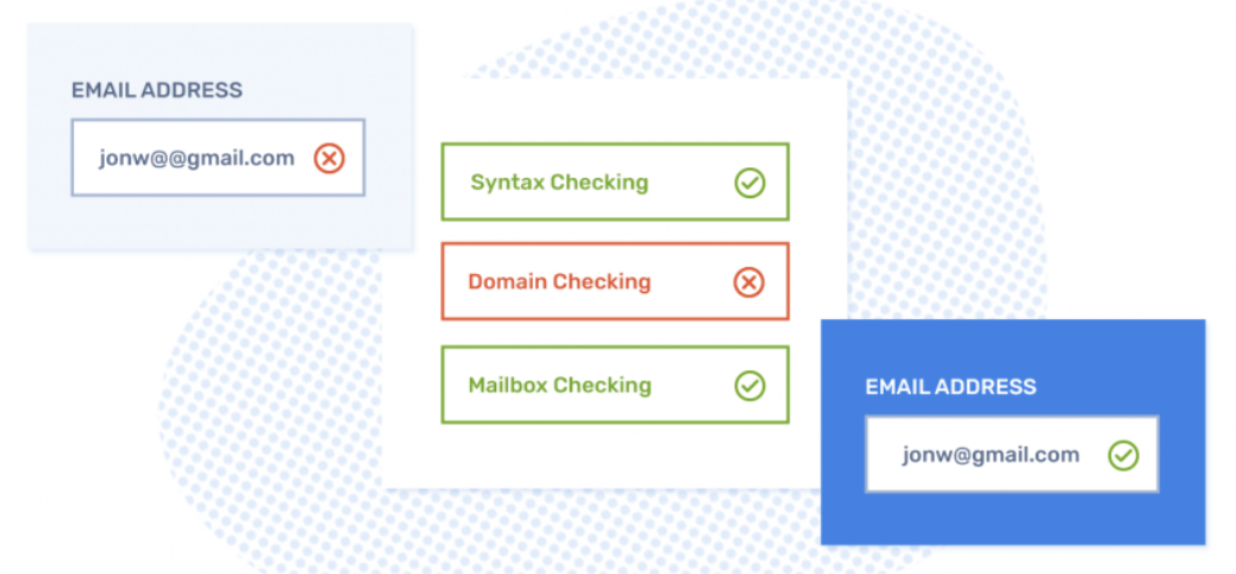
The first thing the email validation service checks is the format of an email address. This simply ensures that the email has all the right information in the right places. It checks for things like missing @ symbols, invalid characters, and out-of-place domain names. This check eliminates entries that are just not actual email addresses due to intentional falsification or misspelling. If you have it configured to do so, this stage is also where unmonitored inboxes like admin and sales emails get filtered out.

### Step 2: Domain Verification

Next, the email validator will check to make sure that the domain is valid and active. This is a matter of looking at the DNS and MX records to ensure that the domain is properly setup and activated, and that the mailbox can receive messages. This is where the correctly formatted, but invalid, emails are removed from the list.

### Step 3: Mailbox Check

This last stage is where the rest of the bad emails get caught. The email validator will contact the mail server through SMTP and find out if the mailbox really exists. This filters out most disposable email addresses.



## **1.3 Admin Portal**

**1. Track sub-merchants**

* 1. Display a list of the sub-merchants who are inactive for 30 days
  2. Display a list of sub-merchants with more than 50% unsuccessful transactions in a month.
  3. Admin should be notified on more than 10% chargebacks of a sub-merchant.
  4. Admin should be notified on fake email registration.
  5. Sub-merchants that have not logged in to the Monay portal for 3 months will be inactivated.
     1. An email will be sent to the sub-merchant for the first two months and two emails after every 15 days for the third month.
     2. If no action is taken by the sub-merchant, the account will be inactivated.

**2. Reports**

Reports can be generated that will help monitor the money flow of the sub-merchant business. One can export all your transaction data, on a daily, monthly, and yearly basis. The reports can either be downloaded as a CSV, or XLS and can be shared through email. Following reports can be generated:

1. Reconciliation Report by Activity Date
2. Reconciliation Report by Settlement Date
3. Chargeback Report by Activity Date
4. Chargeback Report by Settlement Date
5. Declined Transaction Report
6. Convenience Fee Report
7. Monay GPS Fee Report
8. Settlements: This report provides a list of the settlement in the selected time range.
9. Payments: This report provides details of all payments that were created in the selected time range.
10. Combined Report: This report provides all transactions (payments, refunds, adjustments, and transfers) and settlements made in the selected time range.
11. Refunds: This report provides details of all refunds that were initiated in the selected time range.
12. Payment Links Report: This report provides details of all the payment links that were created in the selected time range.

**Reference**

1. <https://www.carat.fiserv.com/content/dam/carat/us/en/pdf/fraud-mitigation.pdf>
2. <https://www.fiserv.com/en-me/solutions/manage-risk-fraud.html>