

User Management service

- **Update Mobile Number**

- **Service Description**

The Update Mobile Number service allows users to change their registered mobile number. The new number is verified via OTP before being updated for all notifications and alerts.

- **General User Story**

"As a wallet user, I want to update my registered mobile number, so that I can continue receiving OTPs, notifications, and important account alerts on my new number."

- **Detailed Update Mobile Number Flow**

keypad only for the customer.

- The user cannot proceed to the OTP verification step unless a valid number is entered. A clear error message must be displayed if the input is invalid or incomplete.

- Negative Scenarios

- Invalid Format:

Step #1

Incorrect or incomplete number → "Please enter a valid phone number."

- Empty Field:

No input provided → "This field is required."

- Duplicate Number:

Number already used → "The phone number is already in use."

- Too Many Attempts: 5+ rapid attempts → "Temporarily blocked. Try again later."
- System Error:

Server failure or internal error
→ "A system error has occurred."
- The system validates the entered number to ensure:
- If the entered mobile number **exists** in the system, a message will appear "Dear customer, we would like to inform you that the mobile number you entered is already registered with another account. Please use a different number. Thank you for choosing Tayseer Finance Company."
- If the entered mobile number **doesn't exist** in the system, they will proceed to the next step, which is **"Mobile OTP."**

<p>Step #2</p>	<p>Mobile OTP</p> <ul style="list-style-type: none"> • A code is sent to the user's mobile number. • If the code is confirmed by the user, they will proceed to the next step, "Tahaquq." • If the code is not confirmed, they will only be allowed to repeat the process (5 times). • If all attempts are completed without the code being entered correctly, the process will stop. • If the user successfully enters the code correctly, they will proceed to the next step, "Tahaquq."
	<p>Tahaquq Service</p> <ul style="list-style-type: none"> • If the mobile number matches the ID number, two messages are sent: <ul style="list-style-type: none"> • To the old mobile number "Dear customer, we would like to inform you that your registered mobile number has been changed from [old mobile number] to [new mobile number] on (DD/MM/YYYY). If you didn't request this change, please contact Tayseer Finance Company immediately."
<p>Step #3</p>	<p>Also in Arabic</p> <p>"عزيزي العميل، نود إبلاغكم بتغيير رقم هاتفك المسجل من [الرقم القديم] إلى [الرقم الجديد] بتاريخ (DD/MM/YYYY). إذا لم تطلب هذا التغيير، يُرجى التواصل مع شركة تيسير للتمويل فوراً."</p> <ul style="list-style-type: none"> • To the new mobile number "Dear customer, we would like to inform you that your mobile number has been successfully updated to [new mobile number] on (DD/MM/

YYYY). Thank you for choosing Tayseer Finance Company."

Also in Arabic

"عزيزي العميل، نود إبلاغكم بتحديث رقم هاتفك بنجاح إلى [الرقم الجديد] بتاريخ / DD/MM/ YYYY. شكرًا لاختيارك شركة تياسير للتمويل."

- **If the mobile number doesn't match the ID number,** the process stops, and an error message is displayed:

"The mobile number you entered doesn't match the ID number in our records. Please check your information and try again."

- **Process-Flow**
[UpdateMobileNumber.pdf](#)
- **Note:**
To change their mobile number, the user must **log in** to the system.
- **Update Email**
- **Service Description:**
The Update Email service allows users to change their registered email address. The new email is verified via OTP or confirmation link before being updated for all communications and alerts.
- **General User Story**
"As a wallet user, I want to update my email address so that I can receive account alerts and notifications on my new email."
- **Detailed Update Email Flow:**

Step #1	New email Address <ul style="list-style-type: none">• The customer enters their email address.
	Email OTP <ul style="list-style-type: none">• A code is sent to the email address

- A code is sent to the email address entered, and then checked.
- If the code is **confirmed** by the user, a message is sent informing them that "**Dear customer, we would like to inform you that the email has been** successfully updated to [new email] **on (DD/MM/YYYY).** **Thank you for choosing Tayseer Finance Company.**"

Also in Arabic

"عزيزي العميل، نود إبلاغكم بتحديث البريد الإلكتروني بنجاح إلى [البريد الإلكتروني الجديد] بتاريخ (DD/MM/YYYY). شكراً لاختيارك شركة تيسير للتمويل."

- If the code is **not confirmed**, they will only be allowed to repeat the process (5 times.)
- If **all attempts are completed without the code being entered correctly**, the process will stop.
- If the user **successfully** enters the code **correctly**, the OTP email will be **reset again, two messages are sent:**
- *To the old email "Dear customer, we would like to inform you that your registered email has been changed from [old email] to [new email] on (DD/MM/YYYY). If you didn't request this change, please contact Tayseer Finance Company immediately."*

• Also in Arabic

"عزيزي العميل، نود إبلاغكم بتحديث البريد الإلكتروني المسجل من [الإيميل القديم] إلى [الإيميل الجديد] بتاريخ (DD/MM/YYYY). إذا لم تطلب هذا التغيير، يرجى التواصل مع شركة تيسير للتمويل فوراً."

Step #2

- **To the new email "Dear customer, we would like to inform you that your email number has been successfully updated to [new email] on (DD/MM/YYYY). Thank you for choosing Tayseer Finance Company."**

- **Also in Arabic**

"عزيزينا العميل، نود إبلاغكم بتحديث البريد الإلكتروني بنجاح إلى [البريد الإلكتروني الجديد] بتاريخ (DD/MM/YYYY). شكرًا لاختيارك شركة تياسير للتمويل."

- **Process-Flow**
UpdateEmail.pdf
- **Note:**
 - If this is the first time the user enters their email address, the process is "**Add Email**".
 - If the email address has already been added and the user wants to update it, the process is "**Update Email**".
- **Update KYB Form**
- **Service Description**

The Update KYB Form service allows users to modify or update their personal information in the KYB form to ensure compliance with regulatory requirements.
- **General User Story**

"As a wallet user, I want to update my KYB information so that my account remains valid and compliant with regulations."
- **Fields Available for Update (as used during onboarding)**
- **Source of Funds =>**
- **Drop-down list:**
- **Sales,**
- **Investments,**
- **Loans, Donations,**
- **Freelance,**
- **Other (with additional text field if selected)**

- ***Expected Transaction Volume and Value =>***
- ***Monthly/Annual estimates of transaction volume and value.***
- **Includes sub-layers (drop-down, one option each):**
- **Expected monthly payroll processing volume and value**
- **Expected monthly domestic transfer volume and value**
- **Expected monthly international transfer volume and value**
- **Expected monthly deposit volume and value**
- ***Purpose of the Digital Wallet Account =>***
- ***Multiple selection field (options such as):***
- ***Receiving payments from customers for services/goods***
- ***Paying suppliers***
- ***Managing petty cash***
- ***Distributing funds***
- ***Receiving disbursements***
- ***Donations***
- ***Other (with additional text field if selected)***
- **Detailed Update KYB Form Flow:**

Step #1	Update KYB Form
	<ul style="list-style-type: none"> • The user updates the KYB Form.

	<p>Mobile OTP / Passcode</p> <ul style="list-style-type: none"> • A code is sent to the user (OTP if the customer is using the portal, or passcode if the customer is using a mobile device). Then, a check is performed: • If the code is confirmed by the user, the customer's risk rating details will be updated. • If the code is not confirmed, they will only be allowed to repeat the process (5 times.) • If all attempts are completed without the code being entered correctly, the process will stop. • If the user successfully enters the code correctly, the customer's risk rating details will be updated.
--	---

- **Process-Flow**
UpdateKYBForm.pdf
- **Change Password/Passcode**
- **Service Description**
The Change Password/Passcode service allows users to update their login password or wallet passcode for enhanced account security.
- **General User Story**
"As a wallet user, I want to change my password/passcode so that I can keep my account secure."
- **Detailed Change Password/Passcode Flow:**

	<p>Change the password/passcode</p> <ul style="list-style-type: none"> • The user selects to change the password/passcode.
--	--

<p>Step #2</p>	<p>Current password/passcode</p> <ul style="list-style-type: none"> • We ask the customer to enter the current password/passcode, based on the customer's choice. The verification process is then performed. • If the user enters it correctly, they will proceed to the next step "Enter a new password/passcode." • If the user enters it incorrectly, they will only be allowed to repeat the process (5 times.) • If all attempts are completed without the password/passcode being entered correctly, the process will stop. • If the user successfully enters the password/passcode correctly, they will proceed to the next step "Enter a new password/ passcode."
	<p>New password/passcode</p> <ul style="list-style-type: none"> • We ask the customer to enter the new password/passcode. And then we ask for confirmation again. • Password – Portal Rules • A complex string of characters used for secure login. • Typically 8+ characters, includes letters, numbers, and symbols. • Strong password policies are enforced in accordance with the identity and access management policy of CHAGHF AL-HALLOUL. • Unused Accounts: All virtual or

Step #3

- **inactive accounts must be suspended or deleted.**
- **Session Management:** Sensitive systems auto-logout sessions after inactivity (recommended timeout: 5 minutes).
- **Multi-Factor Authentication (MFA):** Mandatory for all users, must include at least two of the following:
 - **Biometric (e.g., fingerprint)**
 - **Physical security key**
 - **One-time password (OTP)**
 - **Smart card**
 - **Encryption certificate**
- **Device Access Control:** Access restricted by IP-based access lists and device roles.
- **Passcode – App Rules**
- **A short numeric code used for quick access**
- **5 digits**
- **Mobile app login (fast access to wallet functions)**
- **Medium – relies on simplicity and speed**
- **Sequential numbers are not allowed, such as: 12345 or 23456**
- **Repeated numbers are not allowed, such as: 11111**
- **Reverse or patterned numbers are not allowed, such as: 98765 or 112233**
- **Reusing your previous passcode is not allowed when changing it.**
- **After a certain number of failed**

	<p><i>After a certain number of failed attempts (e.g., 5 times), the app will be temporarily locked.</i></p> <ul style="list-style-type: none"> • The device used for registration is classified as a trusted device.
	<ul style="list-style-type: none"> • On mobile phones, once linked, the user can log in using passcode/biometric. • Multi-Factor Authentication (MFA): Two-factor authentication must be enabled for all users (FIDO2 combines biometric with PIN or password). • Step-up Authentication: Required when performing: <ul style="list-style-type: none"> • Large financial transactions. • Password reset. • Device rebinding. • Session Security: <ul style="list-style-type: none"> • Auto-expire session after inactivity • Forced logout if the app is sent to the background • Account Controls: <ul style="list-style-type: none"> • Disable inactive accounts after a certain period • Refresh password periodically (every specified period) • Lock account after a certain number of failed login attempts

- **Process-Flow**
ChangePasswordPasscode.pdf

- **Enable/Disable Biometrics**

- **Service Description:**

The Enable/Disable Biometrics service allows users to activate or deactivate biometric authentication (such as fingerprint or face recognition) for quick and secure access to the wallet.

- **General User Story**

"As a wallet user, I want to enable or disable biometrics so that I can choose between convenience and security when accessing my wallet."

- **Detailed Enable/Disable Biometrics Flow:**

	Selects enable/disable biometrics access
Step #1	<ul style="list-style-type: none"> • The customer selects to enable/ disable biometrics access according to the current status.
Step #2	<p>Disable Biometrics login</p> <ul style="list-style-type: none"> • If the customer chooses to disable biometrics, it will be disabled.
Step #3	<ul style="list-style-type: none"> • If the customer chooses to enable biometrics, the device will be checked to see if it supports biometrics. • If the device supports biometrics, they will proceed to the next step, "Enter Passcode." • If the device doesn't support biometrics, the process will stop.

Step #4	<p>Enter Passcode</p> <ul style="list-style-type: none"> • The customer enters the passcode. • If the user enters it correctly, biometrics will be enabled, and the process will then end. • If the user enters it incorrectly, they will only be allowed to repeat the process (5 times.) • If all attempts are completed without the passcode being entered correctly, the process will stop. • If the user successfully enters the passcode correctly, biometrics will be enabled, and the process will then end.
---------	--

- **Process-Flow**
[EnableDisableBiometricAccess.pdf](#)
- **Note**
This option **appears** if the device **supports biometric login**. However, if it **doesn't support biometrics, it will not occur**.
- **Notification Management**
- **Service Description:**
The Notification Management service allows users to enable or disable push, email, and marketing notifications according to their preferences.
- **General User Story**
"As a wallet user, I want to manage notifications so that I can choose which alerts I receive."
- **Detailed Notification Management Flow:**

Step #1	<p>disable. We have three types of notifications:</p> <ul style="list-style-type: none"> • Push notifications, • Email notifications, • Marketing notifications.
Step #2	<p>Push Notifications</p> <ul style="list-style-type: none"> • If the customer selects push notifications, the notification will be enabled or disabled. • Note: Push notifications are only available on mobile and are not available on desktop.
Step #3	<p>Email Notifications</p> <ul style="list-style-type: none"> • If the customer selects email notifications, it will be checked whether they actually have an email address. • If they have one, the notifications email will be enabled/disabled. • If they don't have one, they will proceed to the next step, "Add New Email." • asked to add one, and then an OTP email will be sent.
Step #4	<p>Add New Email</p> <ul style="list-style-type: none"> • The customer adds his own email and then proceeds to the next step, "OTP Email."

Step #5	<p>Email OTP</p> <ul style="list-style-type: none"> • A code is sent to the email address entered, and then checked. • If the code is confirmed by the user, email notifications will be enabled/disabled. • If the code is not confirmed, they will only be allowed to repeat the process (5 times.) • If all attempts are completed without the code being entered correctly, the process will stop. • If the user successfully enters the code correctly, the OTP email will be reset again, and email notifications will be enabled/disabled.
Step #6	<p>Marketing Notifications</p> <ul style="list-style-type: none"> • If the customer selects marketing notifications, the notification will be enabled or disabled. • If the customer disables marketing notifications, no further marketing notifications should be sent. • The system should flag the user as opted-out to prevent future marketing messages.

- **Process-Flow**
EnableDisableNotifications.pdf

- Update National Address

- **Service Description**

The Update National Address service allows the user to update their registered national address using their UNN (national number). The system validates the structure of the address, updates it in the profile, and requires OTP/Passcode confirmation to ensure security.

- **General User Story**

“As a wallet user, I want to update my national address using my UNN so that my account records remain accurate and compliant with regulations.”

- **Detailed Flow:**

	Select Update National Address
Step #1	<ul style="list-style-type: none"> • The customer selects update national address.
Step #2	<p>Updates National Address Details</p> <ul style="list-style-type: none"> • The customer updates the national address details.
	<p>Validate National Address Structure</p> <ul style="list-style-type: none"> • The system checks that all fields follow the required format rules. • National Address – Format Rules • Region Must be selected from predefined list (no free text). • City Must be selected from predefined list based on the chosen region. • District Must be selected from predefined list based on the chosen city.

- Street Name

Alphabetic characters only
(Arabic or English letters).

No numbers or special
characters allowed.

Maximum length: 100
characters.

Step #3

- Building Number

Numeric only.

Exactly 4 digits (e.g., 1234).

- Postal Code

Numeric only.

Exactly 5 digits.

- Additional Number (Unit/
Apartment)

Numeric only.

Exactly 4 digits.

	<ul style="list-style-type: none"> • If the National Address is valid, the customer proceeds to the next step “Mobile OTP / Passcode” • If the National Address is invalid, the customer can update their national address details again.
	<p><i>Mobile OTP (Portal) / Passcode (Mobile)</i></p> <ul style="list-style-type: none"> • <i>Mobile OTP (Portal)</i> • <i>A code is sent to the user's mobile number.</i> • <i>If the code is confirmed by the user, the national address will be updated successfully, and the process will be completed.</i> • <i>If the code is not confirmed, they will only be allowed to repeat the process (5 times).</i> • <i>If all attempts are completed without the code being entered correctly, the process will stop.</i> • <i>If the user successfully enters the code correctly, the national address will be updated successfully, and the process will be completed.</i>
Step #4	<ul style="list-style-type: none"> • <i>Passcode (Mobile)</i> • <i>When making a change via the mobile app, the user is prompted to enter their passcode.</i> • <i>If the passcode is confirmed by the user, the national address will be updated successfully, and the process will be completed.</i>

By the user, the national address will be updated successfully, and the process will be completed.

- *If the passcode is not confirmed, they will only be allowed to repeat the process (5 times).*
- *If all attempts are completed without the passcode being entered correctly, the process will stop.*
- *If the passcode is entered correctly, the national address will be updated successfully, and the process will be completed.*

- **Process-Flow**

UpdateNationalAddress.pdf

- **User Limit Management**

- **Notes**

- **Wallet limit management =>** Limits applied to the wallet as a whole (e.g., the daily limit for the entire wallet, regardless of the number of users).

- **User limit management =>** Limits applied to an individual user within a specific user (e.g., the daily limit for a specific user's transactions).

- **This step will be carried out through the user profile, where limits are managed at the user level.**

- **Service Description**

The User Limit Management service allows users to view and track their individual limits, such as daily or monthly transaction and withdrawal limits, which apply specifically to them rather than the overall wallet.

- **Configuration limit at the Overall User**

- **If the customer wants to configure a limit on the overall user activity.**

- **General User Story:**

"As a wallet user, I want to configure daily and monthly transaction limits for my account (User Level), so that I can control my personal usage and avoid exceeding my planned budget."

- **Detailed Flow:**

	Select Overall
Step #1	<ul style="list-style-type: none"> • If the customer wants to configure a limit on the entire user account, select “Overall.”
Step #2	<p>Change overall user limit</p> <ul style="list-style-type: none"> • In this step, the customer changes the amount he wants at the overall user level, covering all wallets and transactions linked to that user
Step #3	<p>Specify new limit (within the allowed range)</p> <ul style="list-style-type: none"> • The configuration must be within the allowed limits at the overall user level, and the initial values should be between 0 - 100,000 SAR.
	<p>Mobile OTP (Portal) / Passcode (Mobile)</p> <ul style="list-style-type: none"> • Mobile OTP (Portal) • A code is sent to the user's mobile number. • If the code is confirmed by the user, the order will succeed, the value will change, and the process will complete. • If the code is not confirmed, they will only be allowed to repeat the process (5 times). • If all attempts are completed without the code being entered correctly the process will

Step #4

...
stop.

- *If the user successfully enters the code correctly, the order will succeed, the value will change, and the process will complete.*
- *Passcode (Mobile)*
- *When making a change via the mobile app, the user is prompted to enter their passcode.*
- *If the passcode is confirmed by the user, the order will succeed, the value will change, and the process will complete.*
- *If the passcode is not confirmed, they will only be allowed to repeat the process (5 times).*
- *If all attempts are completed without the passcode being entered correctly, the process will stop.*
- *If the passcode is entered correctly, the process is successful, the value will change, and the process will complete.*

- *Configuration limit for a specific transaction*
- *If the customer wants to configure a limit for a specific transaction at the user level.*
- *General User Story*
"As a wallet user, I want to configure a spending limit for a

specific transaction at the user level, so that I can ensure I don't spend more than intended on that individual transaction."

- Detailed Flow:

	Select Specific Transaction
Step #1	<ul style="list-style-type: none"> • <i>If the customer wants to configure a limit for a specific transaction, select "Specific Transaction."</i>
Step #2	<p>Change Specific Transaction Limit</p> <ul style="list-style-type: none"> • <i>In this step, the customer changes the amount he wants at a specific transaction level.</i>
Step #3	<p>Selects Transaction</p> <ul style="list-style-type: none"> • <i>The customer selects the transaction whose value he wants to change.</i>
Step #4	<p>Specify a new limit (within the allowed range)</p> <ul style="list-style-type: none"> • <i>The configuration must be within the allowed limits within the wallet, which are determined by the system.</i>
	<p>Mobile OTP (Portal) / Passcode (Mobile)</p> <ul style="list-style-type: none"> • <i>A code is sent to the user's mobile number.</i> • <i>If the code is confirmed by the user, the order will succeed, the value will change, and the process will complete.</i> • <i>If the code is not confirmed, they will only be allowed to repeat the process (5 times).</i> • <i>If all attempts are completed without the code being entered correctly, the process will stop.</i>

Step #5

- *If the user successfully enters the code correctly, the order will succeed, the value will change, and the process will complete.*
- **Passcode (Mobile)**
- *When making a change via the mobile app, the user is prompted to enter their passcode.*
- *If the passcode is confirmed by the user, the order will succeed, the value will change, and the process will complete.*
- *If the passcode is not confirmed, they will only be allowed to repeat the process (5 times).*
- *If all attempts are completed without the passcode being entered correctly, the process will stop.*
- *If the passcode is entered correctly, the process is successful, the value will change, and the process will complete.*

- **Process-Flow for Limits Configuration (Overall , Specific Transaction):**
UserLimitManagement.pdf
- Trusted Devices Management
- **Service Description**
This service allows the customer to view and manage the list of trusted devices linked to their account. The user can deactivate devices or review login history to ensure account security.

- **General User Story**

“As a wallet user, I want to manage my trusted devices (Desktop and Mobile) — including deactivation and review — so that I can ensure only authorized devices have access to my account and maintain better control over my security.”

- **Detailed Flow:**

	Select Device Management
Step #1	<ul style="list-style-type: none"> • <i>The customer selects the device on which he wants to manage the process.</i>
Step #2	<p>Retrieve Device(s) Details</p> <ul style="list-style-type: none"> • <i>This step allows the system to fetch and display the list of devices linked to the user's account. The retrieved details may include device type, operating system, last login date/time, and trust status (trusted or not).</i>
Step #3	<p>Select Device Deactivate</p> <ul style="list-style-type: none"> • <i>This step allows the user to select a device from their list of trusted devices and deactivate it. Deactivating a device prevents it from accessing the user's account.</i>
	<p>Mobile OTP (Portal) / Passcode (Mobile)</p> <ul style="list-style-type: none"> • <i>A code is sent to the user's mobile number.</i> • <i>If the code is confirmed by the user, the process will complete.</i> • <i>If the code is not confirmed, they will only be allowed to repeat the process (5 times).</i> • <i>If all attempts are completed without the code being entered</i>

Step #4

correctly, the process will stop.

- *If the user successfully enters the code correctly, the process will complete.*
- **Passcode (Mobile)**
- *When making a change via the mobile app, the user is prompted to enter their passcode.*
- *If the passcode is confirmed by the user, the order will succeed, the value will change, and the process will complete.*
- *If the passcode is not confirmed, they will only be allowed to repeat the process (5 times).*
- *If all attempts are completed without the passcode being entered correctly, the process will stop.*
- *If the passcode is entered correctly, the process is successful, the value will change, and the process will complete.*

- **Process-Flow**
TrustedDevicesManagement.pdf
- **Preferred Language**
- **Service Description**
The Preferred Language service allows the user to choose or update the

language they prefer to use in the application and for all notifications, enhancing usability and overall customer experience.

- **General User Story**

“As a wallet user, I want to set and update my preferred language so that I can interact with the application and receive notifications in the language I understand best.”

- **Detailed Flow:**

Step #1	<ul style="list-style-type: none">• <i>The user navigates to Settings → Preferred Language.</i>
Step #2	<ul style="list-style-type: none">• <i>The system displays a list of available languages (e.g., Arabic, English; additional languages can be configured based on business requirements).</i>
Step #3	<ul style="list-style-type: none">• <i>The user selects the Preferred language from the list.</i>• <i>The new preferred language is saved in the user profile.</i>
Step #4	<p><i>Once updated:</i></p> <ul style="list-style-type: none">• <i>The application interface is immediately adjusted to the chosen language.</i>• <i>Future notifications and communications (SMS, email, push notifications) will be sent in the selected language.</i>• <i>A confirmation message is displayed to the user indicating that the language preference has been updated successfully.</i>

