

## BRD - Digital Wallet Project

### ❖ Scope (in general):

The digital wallet is being developed in two main phases:

#### - **Phase 1: B2B – Institutional Wallet (Current Focus)**

This phase targets businesses, aiming to enable organizations to manage their financial operations efficiently through a secure digital wallet account.

- Key Features of the B2B Wallet:

- Open a wallet account for your business
- Manage transactions and balances
- Pay bills
- Local money transfers
- Top up wallet
- Receive incoming remittances
- Issue cards and payments

#### - **Phase 2: B2C —Employee Wallet (Later)**

In the next phase, the focus will shift to individual users (employees) to enable personal financial services through their wallet accounts.

### ❖ Services Overview

#### 1. **Onboarding Service “Sole Proprietorship, Individual owner company”**

##### \* **Service Description:**

- Onboarding is the process that allows a new user to register themselves in the system as a representative of a sole proprietorship (Single Owner).
- The primary objective is to verify the user's identity and business data to ensure compliance with legal and regulatory standards before allowing them to use the e-wallet.
- This process includes verifying:
  - Business-type survey
  - Mobile number
  - OTP validation
  - UNN number or ID number
  - Data matching with local and global lists

- Owner authority
- Authorization
- KYB Form
- Set password and account creation
- Biometric setup

**\* General User Story:**

"As a new user, I would like to register my sole proprietorship, through a series of digital verification steps, so that I can use the wallet services."

**\* Detailed Onboarding Flow:**

Step #1	<p>The client will see a survey containing four types of business accounts:</p> <ul style="list-style-type: none"> <li>- <b>Sole Proprietorship</b></li> <li>- <b>Individual owner company</b></li> <li>- <b>Freelancer</b></li> <li>- <b>Multi-Owner Company</b></li> </ul> <ol style="list-style-type: none"> <li>1. If the client selects (sole proprietorship, individual owner company, or freelancer), the onboarding process continues, and they move to the next step, which is entering their mobile number.</li> <li>2. If the client selects (multi-owner company), the onboarding process stops, and they will see the message, "Sorry, we don't support opening accounts of this type."</li> <li>3. The user chooses to register as a <b>sole proprietorship or an individually owned company</b></li> </ol>
Step #2	<p><b>Mobile Number Entry</b> The user enters their mobile number</p> <p><b>Acceptance Criteria:</b></p> <ul style="list-style-type: none"> <li>- The user must enter a valid local Saudi phone number that starts with (05) and consists of exactly 10 digits (numbers only, no letters), with support for both Arabic and English numerals.</li> <li>- The system automatically converts Arabic numerals to English.</li> <li>- The system must verify that the phone number is not</li> </ul>

	<p>already associated with another user account.</p> <ul style="list-style-type: none"> <li>- The system must display the digit keypad only for the customer.</li> <li>- 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.</li> </ul> <p><b>Negative Scenarios</b></p> <ul style="list-style-type: none"> <li>- Invalid Format: Incorrect or incomplete number → "Please enter a valid phone number."</li> <li>- Empty Field: No input provided → "This field is required."</li> <li>- Duplicate Number: Number already used → "The phone number is already in use."</li> <li>- Too Many Attempts: 5+ rapid attempts → "Temporarily blocked. Try again later."</li> <li>- System Error: Server failure or internal error → "A system error has occurred."</li> </ul>
Step #3	<p><b>OTP Verification</b></p> <p><b>Acceptance Criteria:</b></p> <ul style="list-style-type: none"> <li>- System sends OTP to the phone number immediately after entry, with a dedicated input field for the code.</li> <li>- Code expires after 5 minutes.</li> <li>- "Resend Code" option becomes available after 1 minute.</li> <li>- If five failed code attempts are made, the process is terminated and a temporary session lock is applied (for example).</li> <li>- If successful, a "Success" message appears upon correct entry, and the user proceeds to the CR-UNN step.</li> </ul>

	<p><b>Negative Scenarios:</b></p> <ul style="list-style-type: none"> <li>- The user enters an incorrect OTP → The message "Invalid code, try again" is displayed.</li> <li>- The user enters an expired code → The message "The code has expired, try again" is displayed.</li> <li>- The user enters the code too late after it expires → Verification is prevented with the message "Invalid code".</li> <li>- The user doesn't receive the code due to an SMS issue → The message "The option to resend the code after 30 seconds" is displayed.</li> <li>- The user attempts to enter more than 3 incorrect code → The session is temporarily closed with the message "Too many attempts, try again later."</li> <li>- The user enters the correct code, but there is an internal error → The message "An error occurred, please try again later" is displayed.</li> </ul> <p>The business should have the ability to modify any error message text through a designated interface in the business portal without requiring technical intervention.</p>
Step #4	<p><b>CR/UNN Entry</b></p> <ul style="list-style-type: none"> <li>- The user enters the UNN (national number). This company number is then searched for using "Stitch", which is primarily linked to Arab Bank. Feedback is then sent to us.             <ol style="list-style-type: none"> <li>1. If the CR/UNN number matches and is blacklisted, the process stops.</li> <li>2. If the CR/UNN number not match, the user proceeds to the next step, "Wathiq"</li> </ol> </li> <li>- An API Call is connected to Stitch when the search is executed.</li> <li>- Caching is used to save data after the search process, so that if there is a mismatch and the customer refuses to complete the process, if he enters this wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning. Additionally, the caching mechanism should be configurable,</li> </ul>

	and initially, the cache duration for the CR Details Service should be <b>set to 1 month</b> .
Step #5	<p><b>Wathiq Verification "External Services"</b></p> <ul style="list-style-type: none"> <li>- Wathiq will be primarily linked to Stitch, which retrieves the required CR/UNN data, such as the company name, company establishment, and other information. It then performs a data check.</li> </ul> <ol style="list-style-type: none"> <li>1. Business Activity Check: <ul style="list-style-type: none"> <li>- The business activity must not be listed in the internal blocked activities list.</li> <li>- If the activity is found in the blocked list → the process must be stopped.</li> </ul> </li> <li>2. Business Type Check: <ul style="list-style-type: none"> <li>- The business type must be either an individual establishment or a single owner.</li> <li>- Any other business types should be rejected, and the process should not proceed to global screening.</li> </ul> </li> </ol> <ul style="list-style-type: none"> <li>- The CR/UNN data is checked by a "Global List" (for example, check of the company name, etc.), which is linked to the "External Service (Mozon)", which performs a full data check.</li> </ul> <ol style="list-style-type: none"> <li>1. If a match is found (i.e., this person is suspected), the data is transferred to a "Compilation Review" (manual review within the system). This is where the decision is made whether the person is rejected or accepted. <ul style="list-style-type: none"> <li>- In case of rejection, we have an "internal list" so that if a customer attempts to enter an UNN, it will be invalid, and a text message and an immediate notification will be sent to the user stating, "Sorry, your registration request has been rejected." The UNN has been internally blocked.</li> <li>- If the case is <b>accepted</b> by Compliance Review, a text message and an immediate notification will be sent to the user stating, "<b>Approved, you may now continue your registration.</b>" Then, the user will proceed to "Enter ID Number."</li> </ul> </li> <li>2. If there is no match (i.e., the person is not a suspect), proceed to the next step, which is to "Enter the ID number."</li> </ol>

	<ul style="list-style-type: none"> <li>- The compliance review is done through a third-party "External Portal," and feedback is sent to the system, and based on that, it is determined whether the user can complete the operations or terminate them.</li> <li>- <b>Caching</b> is used to save data after the search process, so that if there is a mismatch and the customer refuses to complete the process, if he enters the wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning.</li> </ul>
Step #6	<p><b>ID Number</b></p> <ul style="list-style-type: none"> <li>- The user must enter a valid ID number starting with (1) or (2) and consisting of exactly 10 digits (with support for Arabic and English numbers)</li> <li>- Among the information provided by the CR/UNN is the ID number of the company's authorized person, such as the administrator or owner. At the same time, the user enters their own ID number.</li> </ul> <ol style="list-style-type: none"> <li>1. If the ID number matches the ID-CR, the process is completed and the user moves to the next step.</li> <li>2. If the ID number not match the ID-CR, the process stops and an error message appears: "Please enter a valid number."</li> </ol>
Step #7	<p><b>Owner ID Screening (Local List) "External Services"</b></p> <ul style="list-style-type: none"> <li>- At this stage, the ID number entered by the user is verified to see if it is on the blacklist. <ol style="list-style-type: none"> <li>1. If there is a match, the process ends.</li> <li>2. If there is no match, the process proceeds to the next stage, "Tahaquq."</li> </ol> </li> <li>- The external "Stitch" service handles the verification process.</li> <li>- Caching is used to save data after the search process for <b>only one month</b>, so that if there is a mismatch and the customer refuses to complete the process, if he enters the wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning.</li> </ul>

Step #8	<p><b>Tahaquq verification "External Services"</b></p> <ul style="list-style-type: none"> <li>- Tahaquq service that links the user's initially entered mobile number with the ID number they also entered.</li> <li>- The owner must be the same as the owner of the entered mobile number for the process to be successful.             <ol style="list-style-type: none"> <li>1. If there is a match between the mobile number and the ID number, the next step is "Nafath Authentication."</li> <li>2. If there is no match, the process is stopped and the message "Mobile number doesn't match ID" appears.</li> </ol> </li> <li>- Caching is used to save data after the search process for 15 days, so that if there is a mismatch and the customer refuses to complete the process, if he enters the wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning.</li> </ul>
Step #9	<p><b>Nafath "External Services"</b></p> <ul style="list-style-type: none"> <li>- The <b>Nafath app</b> will be linked to verify the user. The process is completed by displaying a specific number <b>generated</b> by Nafath to the user. When the user clicks "Go to Nafath" on the interface, they are directed to an <b>external application</b>, "Nafath app".</li> <li>- The user selects the number previously displayed to them, and the feedback is sent to us, either success or failure.</li> <li>- Feedback:             <ol style="list-style-type: none"> <li>1. If the process is complete, the customer proceeds to the next step.</li> <li>2. If the process is not complete, there are two scenarios:                 <ul style="list-style-type: none"> <li>- Rejected, and the Process ended.</li> <li>- The number expired. Here, the customer is presented with another generated number and asked to enter it again.</li> </ul> </li> </ol> </li> </ul>
Step #10	<p><b>Owner Screening (Global List) "External Services"</b></p> <ul style="list-style-type: none"> <li>- Based on the data retrieved from "Authentication Nafath," this data is taken, and part of it is sent to "Global Screening"</li> </ul>

	<p>via an external system, which sends feedback.</p> <ol style="list-style-type: none"> <li>1. If there is a match, the data is transferred to "Compliance Review" (a manual review within the system). Here, the decision is made to reject or accept the person. <ul style="list-style-type: none"> <li>- In the case of <b>rejection</b>, we have an "internal list" so that if the customer attempts to enter an invalid confirmation number again, a text message and a immediate notification will be sent to the user stating, <b>"Sorry, your registration request has been rejected."</b> The process will be stopped."</li> <li>- In the case of <b>accepted</b> by Compliance Review, a text message and an immediate notification will be sent to the user stating, <b>"Approved, you may now continue your registration."</b> Then, the user will proceed to "KYB Form."</li> </ul> </li> <li>2. If there is no match, they will proceed to the next step, "KYB Form."</li> </ol>
Step #11	<p><b>KYB Form - Know Your Business</b></p> <ul style="list-style-type: none"> <li>- In this step, the user fills out the KYB form, which contains company data, such as annual revenue, expected number of transactions, and business activity classification. Based on this data, the system calculates and assigns a specific Risk Rating to the client based on the configuration that the compliance review will later build.</li> <li>- "KYB" form, which includes the following information: <ol style="list-style-type: none"> <li>1. <b>Source of Funds</b> <ul style="list-style-type: none"> <li>- This field is used to determine where the client's primary operating capital (company or business) comes from. It helps assess the client's risk and understand the nature of the funds flowing into the e-wallet.</li> <li>- The field type will be a <b>drop-down list</b> that appears to the client and contains several options, such as: (sales, investments, loans, donations, freelance, Other)</li> <li>- When <b>"Other"</b> is selected, an additional text field appears for manually entering the source.</li> </ul> </li> </ol> </li> </ul>



- This can be adjusted according to the business requirements and targeted segments that management should establish.

## 2. Expected Transaction Volume and Value

- In this field, customers are asked to provide a **monthly/annual** estimate of the volume and value of transactions they will conduct through the wallet. This helps the company understand customer behavior and set appropriate usage limits from the outset.
- This estimate should also include **sub-layers** to be filled out by the customer in the form of a drop-down list.
- Sub-layers:
  - 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.
- Each field type/ **Drop-down list** - one option only.
- Example:

Less than 500,000
500,000 to 1,000,000
1,000,000 to 2,500,000
2,500,000 to 5,000,000
5,000,000 to 20,000,000
20,000,000 to 40,000,000
More than 40,000,000

## 3. Purpose of the Digital Wallet Account:

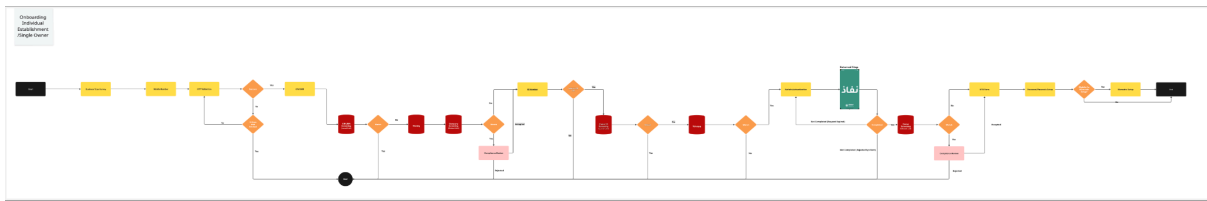
- This field is used to understand how the business will utilize the e-wallet, helping to determine the most suitable services for the customer.

	<ul style="list-style-type: none"> <li>- This field will appear as a <b>Multiple Selection</b> field containing various options, such as: <ul style="list-style-type: none"> <li>• Receiving payments from customers for services/goods</li> <li>• Paying suppliers</li> <li>• Managing petty cash</li> <li>• Distributing funds</li> <li>• Receiving disbursements</li> <li>• Donations</li> <li>• Other</li> </ul> </li> <li>- When "<b>Other</b>" is selected, an additional text field appears for manually entering the source.</li> <li>- This can be adjusted according to the business requirements and targeted segments that management should establish.</li> <li>- Risk Rating for the client is done by "External services Mozon"</li> <li>- Caching is used to save data after a search operation.</li> </ul>
Step #12	<p><b>Set password</b></p> <ul style="list-style-type: none"> <li>- The user creates their own password and then confirms it again.</li> </ul> <p><b>Password - Portal</b></p> <ul style="list-style-type: none"> <li>- A complex string of characters used for secure login</li> <li>- Typically 8+ characters, includes letters, numbers, and symbols.</li> <li>- Web portal login (business dashboard, admin access)</li> <li>- Strong password policies are often enforced</li> </ul> <p><b>Authentication and Access Control Rules</b></p> <ol style="list-style-type: none"> <li>1. Password Policy: <ul style="list-style-type: none"> <li>- The application must enforce the use of complex passwords in accordance with the identity and access management policy of CHAGHF AL-HALLOUL.</li> </ul> </li> <li>2. Session Management: <ul style="list-style-type: none"> <li>- Sensitive systems should auto-logout sessions after inactivity (recommended timeout: 5 minutes).</li> </ul> </li> </ol>


	<p>3. Multi-Factor Authentication (MFA):</p> <ul style="list-style-type: none"> <li>- MFA is mandatory for all users and must include at least two of the following factors: <ul style="list-style-type: none"> <li>• Biometric (e.g., fingerprint)</li> <li>• Physical security key</li> <li>• One-time password (OTP)</li> <li>• Smart card</li> <li>• Encryption certificate</li> </ul> </li> </ul> <p>4. Device Access Control:</p> <ul style="list-style-type: none"> <li>- Access to web applications must be restricted by IP-based access lists and device roles.</li> </ul> <p>5. Unused Accounts:</p> <ul style="list-style-type: none"> <li>- All virtual or inactive accounts must be suspended or deleted.</li> </ul> <p><b>Passcode - App</b></p> <ul style="list-style-type: none"> <li>- The user creates and confirms a password to log in to the app, they then <b>create a passcode</b>. <ul style="list-style-type: none"> <li>- A short numeric code used for quick access</li> <li>- 5 digits</li> <li>- Mobile app login (fast access to wallet functions)</li> <li>- Medium – relies on simplicity and speed</li> <li>- Sequential numbers are not allowed, such as: 12345 or 23456</li> <li>- Repeated numbers are not allowed, such as: 11111</li> <li>- Reverse or patterned numbers are not allowed, such as: 98765 or 112233</li> <li>- Reusing your previous passcode is not allowed when changing it</li> </ul> </li> <li>- After a certain number of failed attempts (e.g., 5 times), the app will be temporarily locked.</li> <li>- When a customer enters a <b>passcode</b> in the app, the device from which they entered the password is linked to the customer via a personal identification number (PIN). This step results in: <ul style="list-style-type: none"> <li>• The device used for registration is classified as a trusted device.</li> <li>• On mobile phones, the device is linked, and the user can use the passcode/ Biometric to log in later.</li> </ul> </li> </ul>
--	--

	<p><b>Device Authentication and Passcode Rules</b></p> <ol style="list-style-type: none"> <li>1. Multi-Factor Authentication (MFA) <ul style="list-style-type: none"> <li>- Two-factor authentication must be enabled for all users.</li> <li>- FIDO2: Combines a fingerprint or face (biometric) with a PIN or password.</li> <li>- Used when logging into the app.</li> </ul> </li> <li>2. Step-up Authentication <ul style="list-style-type: none"> <li>- Additional authentication is required when performing any of the following: <ul style="list-style-type: none"> <li>• Large financial transactions.</li> <li>• Password reset.</li> <li>• Device rebinding.</li> </ul> </li> </ul> </li> <li>3. Session Security <ul style="list-style-type: none"> <li>- Automatically expires the session after a period of inactivity.</li> <li>- Forced logout if the app is sent to the background.</li> </ul> </li> <li>4. Account Controls <ul style="list-style-type: none"> <li>- Disable inactive accounts after a certain period.</li> <li>- Refresh the password periodically (every specified period).</li> <li>- Lock the account after a certain number of failed login attempts.</li> </ul> </li> </ol>
Step #13	<p><b>Biometric Login (It will be explained later)</b></p> <ul style="list-style-type: none"> <li>- Biometric Login allows users to securely access the mobile app using their fingerprint or facial recognition, providing a faster and more secure login experience.</li> </ul> <ol style="list-style-type: none"> <li>1. If the device supports biometric authentication: Enable the "Biometric Setup"</li> <li>2. If the device doesn't support biometric authentication, the process will end.</li> </ol>

## ❖ Onboarding Process-Flow:



- Note: You can also access the file via the following link:

 [Onboarding Process\\_Flow\\_SMEs\\_V2.pdf](#)

## 2. Onboarding Service “Freelancer”:

### \* Service Description:

- Onboarding is the process that allows a new user to register themselves in the system as a representative of a freelancer.
- The primary objective is to verify the user's identity and business data to ensure compliance with legal and regulatory standards before allowing them to use the e-wallet.
- This process includes verifying:
  - Business-type survey
  - Mobile number
  - OTP validation
  - Freelancer License Number or ID number
  - Data matching with local and global lists
  - Owner authority
  - Authorization
  - KYB Form
  - Set password and account creation
  - Biometric setup

### \* General User Story:

"As a new user, I would like to register as a freelancer through a series of digital verification steps, so that I can use the wallet services."

## \* Detailed Onboarding Flow:

Step #1	<p>The client will see a survey containing four types of business accounts:</p> <ul style="list-style-type: none"> <li>- <b>Sole Proprietorship</b></li> <li>- <b>Individual owner company</b></li> <li>- <b>Freelancer</b></li> <li>- <b>Multi-Owner Company</b></li> </ul> <ol style="list-style-type: none"> <li>1. If the client selects (sole proprietorship, individual owner company, or freelancer), the onboarding process continues, and they move to the next step, which is entering their mobile number.</li> <li>2. If the client selects (multi-owner company), the onboarding process stops, and they will see the message, "Sorry, we don't support opening accounts of this type."</li> <li>3. The user chooses to register as <b>a freelancer</b>.</li> </ol>
Step #2	<p><b>Mobile Number Entry</b> The user enters their mobile number</p> <p><b>Acceptance Criteria:</b></p> <ul style="list-style-type: none"> <li>- The user must enter a valid local Saudi phone number that starts with (05) and consists of exactly 10 digits (numbers only, no letters), with support for both Arabic and English numerals.</li> <li>- The system automatically converts Arabic numerals to English.</li> <li>- The system must verify that the phone number is not already associated with another user account.</li> <li>- 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.</li> </ul> <p><b>Negative Scenarios</b></p> <ul style="list-style-type: none"> <li>- Invalid Format: Incorrect or incomplete number → "Please enter a valid phone number."</li> <li>- Empty Field: No input provided → "This field is required."</li> <li>- Duplicate Number:</li> </ul>

	<p>Number already used → "The phone number is already in use."</p> <ul style="list-style-type: none"> <li>- Non-Numeric Input: Letters entered → "Please enter numbers only."</li> <li>- Too Many Attempts: 5+ rapid attempts → "Temporarily blocked. Try again later."</li> <li>- Wrong Country Prefix: Number without Saudi prefix → Transaction blocked</li> <li>- System Error: Server failure or internal error → "A system error has occurred."</li> </ul>
Step #3	<p><b>OTP Verification</b></p> <p><b>Acceptance Criteria:</b></p> <ul style="list-style-type: none"> <li>- System sends OTP to the phone number immediately after entry, with a dedicated input field for the code.</li> <li>- Code expires after 5 minutes.</li> <li>- "Resend Code" option becomes available after 30 seconds.</li> <li>- If three failed code attempts are made, the process is terminated and a temporary session lock is applied (for example).</li> <li>- If successful, a "Success" message appears upon correct entry, and the user proceeds to the <b>Freelancer License No.</b> step.</li> </ul> <p><b>Negative Scenarios:</b></p> <ul style="list-style-type: none"> <li>- The user enters an incorrect OTP → The message "Invalid code, try again" is displayed.</li> <li>- The user enters an expired code → The message "The code has expired, try again" is displayed.</li> <li>- The user enters the code too late after it expires → Verification is prevented with the message "Invalid code".</li> <li>- The user doesn't receive the code due to an SMS issue → The message "The option to resend the code after 30 seconds" is displayed.</li> </ul>

	<ul style="list-style-type: none"> <li>- The user attempts to enter more than 3 incorrect code → The session is temporarily closed with the message "Too many attempts, try again later."</li> <li>- The user enters the correct code, but there is an internal error → The message "An error occurred, please try again later" is displayed.</li> </ul>
Step #4	<p><b>Freelancer License Number</b></p> <ul style="list-style-type: none"> <li>- The user enters the freelancer license number. This number is then searched through the HRSD database "<b>External service</b>", which returns the freelancer's data. Feedback is then sent to us.             <ol style="list-style-type: none"> <li>1. If the freelance license number is not registered in our database, the process stops.</li> <li>2. If the freelance license number is registered in our database, the user proceeds to the next step, "ID number."</li> </ol> </li> </ul>
Step #5	<p><b>ID Number</b></p> <ul style="list-style-type: none"> <li>- The user enters his ID number,</li> </ul>
Step #6	<p><b>Freelancer Screening (Local List) "External Services"</b></p> <ul style="list-style-type: none"> <li>- At this stage, the ID number entered by the user is verified to see if it is on the blacklist.             <ol style="list-style-type: none"> <li>1. If there is a match, the process ends.</li> <li>2. If there is no match, the process proceeds to the next stage, "Tahaquq."</li> </ol> </li> <li>- The external "Stitch" service handles the verification process.</li> <li>- Caching is used to save data after the search process, so that if there is a mismatch and the customer refuses to complete the process, if he enters the wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning.</li> </ul>



Step #7	<p><b>Tahaquq verification "External Services"</b></p> <ul style="list-style-type: none"> <li>- Tahaquq service that links the user's initially entered mobile number with the ID number they also entered.</li> <li>- The owner must be the same as the owner of the entered mobile number for the process to be successful. <ol style="list-style-type: none"> <li>1. If there is a match between the mobile number and the ID number, the next step is "Nafath Authentication."</li> <li>2. If there is no match, the process is stopped and the message "Mobile number doesn't match ID" appears.</li> </ol> </li> <li>- Caching is used to save data after the search process, so that if there is a mismatch and the customer refuses to complete the process, if he enters the wrong option again, he will be blocked from the beginning of the process without the need to repeat the process from the beginning.</li> </ul>
Step #8	<p><b>Nafath "External Services"</b></p> <ul style="list-style-type: none"> <li>- The <b>Nafath app</b> will be linked to verify the user. The process is completed by displaying a specific number <b>generated</b> by Nafath to the user. When the user clicks "Go to Nafath" on the interface, they are directed to an <b>external application</b>, "Nafath app".</li> <li>- The user selects the number previously displayed to them, and the feedback is sent to us, either success or failure.</li> <li>- Feedback: <ol style="list-style-type: none"> <li>1. If the process is complete, the customer proceeds to the next step.</li> <li>2. If the process is not complete, there are two scenarios: <ul style="list-style-type: none"> <li>- Rejected, and the Process ended.</li> <li>- The number expired. Here, the customer is presented with another generated number and asked to enter it again.</li> </ul> </li> </ol> </li> </ul>
Step #9	<p><b>Freelancer Screening (Global List) "External Services"</b></p> <ul style="list-style-type: none"> <li>- Based on the data retrieved from "Authentication Nafath," this data is taken, and part of it is sent to "Global Screening"</li> </ul>

	<p>via an external system, which sends feedback.</p> <ol style="list-style-type: none"> <li>1. If there is a match, the data is transferred to "Compliance Review" (a manual review within the system). Here, the decision is made to reject or accept the person. <ul style="list-style-type: none"> <li>- In the case of <b>rejection</b>, we have an "internal list" so that if the customer attempts to enter an invalid confirmation number again, they will be stopped before the process can begin.</li> <li>- In the case of <b>accepted</b> through the "compliance review", a "success" notification will be sent to the user. You can complete the next steps. After that, the user will be directed to the "KYB Form."</li> </ul> </li> <li>2. If there is no match, they will proceed to the next step, "KYB Form."</li> </ol>
<b>Step #10</b>	<p><b>KYB Form - Know Your Business (It will be changed later)</b></p> <ul style="list-style-type: none"> <li>- In this step, the user fills out the KYB form, which contains company data, such as annual revenue, expected number of transactions, and business activity classification. Based on this data, the system calculates and assigns a specific Risk Rating to the client based on the configuration that the compliance review will later build.</li> <li>- "KYB" form, which includes the following information: <ol style="list-style-type: none"> <li><b>1. Source of Funds</b> <ul style="list-style-type: none"> <li>- This field is used to determine where the client's primary operating capital (company or business) comes from. It helps assess the client's risk and understand the nature of the funds flowing into the e-wallet.</li> <li>- The field type will be a <b>drop-down list</b> that appears to the client and contains several options, such as: (sales, investments, loans, donations, freelance, Other)</li> <li>- When <b>"Other"</b> is selected, an additional text field appears for manually entering the source.</li> <li>- This can be adjusted according to the business requirements and targeted segments that management should establish.</li> </ul> </li> </ol> </li> </ul>

## 2. Expected Transaction Volume and Value

- In this field, customers are asked to provide a **monthly/annual** estimate of the volume and value of transactions they will conduct through the wallet. This helps the company understand customer behavior and set appropriate usage limits from the outset.
- This estimate should also include **sub-layers** to be filled out by the customer in the form of a drop-down list.
- Sub-layers:
  - 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.
- Each field type/ **Drop-down list** - one option only.
- Example:

Less than 500,000
500,000 to 1,000,000
1,000,000 to 2,500,000
2,500,000 to 5,000,000
5,000,000 to 20,000,000
20,000,000 to 40,000,000
More than 40,000,000

## 3. Purpose of the Digital Wallet Account:

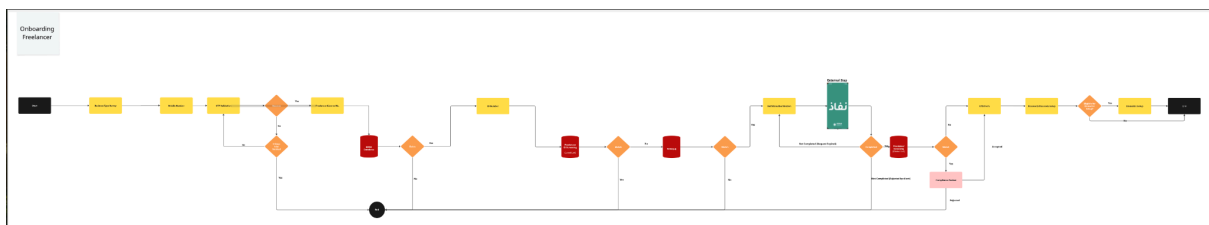
- This field is used to understand how the business will utilize the e-wallet, helping to determine the most suitable services for the customer.

	<ul style="list-style-type: none"> <li>- This field will appear as a <b>Multiple Selection</b> field containing various options, such as: <ul style="list-style-type: none"> <li>● Receiving payments from customers for services/goods</li> <li>● Paying suppliers</li> <li>● Managing petty cash</li> <li>● Distributing funds</li> <li>● Receiving disbursements</li> <li>● Donations</li> <li>● Other</li> </ul> </li> <li>- When "<b>Other</b>" is selected, an additional text field appears for manually entering the source.</li> <li>- This can be adjusted according to the business requirements and targeted segments that management should establish.</li> <li>- Risk Rating for the client is done by "External services Mozon"</li> <li>- Caching is used to save data after a search operation.</li> </ul>
Step #11	<p><b>Set a Password</b></p> <ul style="list-style-type: none"> <li>- The user creates their own password and then confirms it again.</li> </ul> <p><b>Password - Portal</b></p> <ul style="list-style-type: none"> <li>- A complex string of characters used for secure login</li> <li>- Typically 8+ characters, includes letters, numbers, and symbols.</li> <li>- Web portal login (business dashboard, admin access)</li> <li>- Strong password policies are often enforced.</li> </ul> <p><b>Authentication and Access Control Rules</b></p> <ol style="list-style-type: none"> <li>1. Password Policy: <ul style="list-style-type: none"> <li>- The application must enforce the use of complex passwords in accordance with the identity and access management policy of CHAGHF AL-HALLOUL.</li> </ul> </li> <li>2. Session Management: <ul style="list-style-type: none"> <li>- Sensitive systems should auto-logout sessions after inactivity (recommended timeout: 5 minutes).</li> </ul> </li> </ol>


	<p>3. Multi-Factor Authentication (MFA):</p> <ul style="list-style-type: none"> <li>- MFA is mandatory for all users and must include at least two of the following factors: <ul style="list-style-type: none"> <li>• Biometric (e.g., fingerprint)</li> <li>• Physical security key</li> <li>• One-time password (OTP)</li> <li>• Smart card</li> <li>• Encryption certificate</li> </ul> </li> </ul> <p>4. Device Access Control:</p> <ul style="list-style-type: none"> <li>- Access to web applications must be restricted by IP-based access lists and device roles.</li> </ul> <p>5. Unused Accounts:</p> <p>All virtual or inactive accounts must be suspended or deleted.</p> <p><b>Passcode - App</b></p> <ul style="list-style-type: none"> <li>- A short numeric code used for quick access</li> <li>- 5 digits</li> <li>- Mobile app login (fast access to wallet functions)</li> <li>- Medium – relies on simplicity and speed</li> <li>- Sequential numbers are not allowed, such as: 12345 or 23456</li> <li>- Repeated numbers are not allowed, such as: 11111</li> <li>- Reverse or patterned numbers are not allowed, such as: 98765 or 112233</li> <li>- Reusing your previous passcode is not allowed when changing it</li> </ul> <ul style="list-style-type: none"> <li>- After a certain number of failed attempts (e.g., 5 times), the app will be temporarily locked.</li> <li>- When a customer enters a <b>passcode</b> in the app, the device from which the password was entered is linked to the client via a PIN code.</li> </ul> <p><b>Device Authentication and Passcode Rules</b></p> <p>1. Multi-Factor Authentication (MFA)</p> <ul style="list-style-type: none"> <li>- Two-factor authentication must be enabled for all users.</li> <li>- FIDO2: Combines a fingerprint or face (biometric) with a PIN or password.</li> <li>- Used when logging into the app.</li> </ul>
--	---

	<p>2. Step-up Authentication</p> <ul style="list-style-type: none"> <li>- Additional authentication is required when performing any of the following: <ul style="list-style-type: none"> <li>• Large financial transactions.</li> <li>• Password reset.</li> <li>• Device rebinding.</li> </ul> </li> </ul> <p>3. Session Security</p> <ul style="list-style-type: none"> <li>- Automatically expires the session after a period of inactivity.</li> <li>- Forced logout if the app is sent to the background.</li> </ul> <p>4. Account Controls</p> <ul style="list-style-type: none"> <li>- Disable inactive accounts after a certain period.</li> <li>- Refresh the password periodically (every specified period).</li> <li>- Lock the account after a certain number of failed login attempts.</li> </ul>
Step #12	<p><b>Biometric Login (It will be explained later)</b></p> <ul style="list-style-type: none"> <li>- Biometric Login allows users to securely access the mobile app using their fingerprint or facial recognition, providing a faster and more secure login experience.</li> </ul> <ol style="list-style-type: none"> <li>1. If the device supports biometric authentication: Enable the "Biometric Setup"</li> <li>2. If the device doesn't support biometric authentication, the process will end.</li> </ol>

#### ❖ Onboarding Process-Flow:



- Note: You can also access the file via the following link:

 [Onboarding\\_Freelancers\\_V2.pdf](#)