

By using a 2-way authenticator to communicate to whoever is logging in, we can prevent someone from using someone else's account to make payments for them. There are no alternatives to this, and the only tradeoff is if the user doesn't have access to a way to authenticate the login, they will have to make a new account.

To prevent payment conflicts or users registering multiple times, a one-time secret code request should be made before the payment process. The user should be asked which method they prefer to receive the code, either through a text message or an email. Once the code is confirmed, the user can proceed to the payment process. In this case, the system provides the user with a one-time secret code that must be entered to complete the payment process. The code is usually sent to the user via text message or email. After the confirmation of the code, the user converts to the payment process. By doing so, payment conflicts between two users who have used a similar ID or account are prevented because each secret code can only be used once.

Additionally, if the user has already registered, the text message or email containing the secret code is only sent to the phone number or email address that is registered in the system. As a result, this method is highly secure and effective in preventing fraud and payment conflicts.