Section A: Scope of Work Summary

**Business Requirements:**

1. For fraud detection, on the 3rd step up authentication at the same day, change user account to lock status under suspected fraud. Customers need to call support to unblock.
2. If customer increase limit today, if customer do open transfer or use today's created favourite account, change user account to lock status under suspected fraud. Customers need to call support to unblock.

**Scope of Changes:**

1. **3rd “step up authentication”.**
	1. Add new “Step-up Authentication” frequency parameter in the UPASS Config table
	2. Add new field in CORUS for the parameter maintenance under Password Configuration Management
	3. Add logic to store user’s “Step-up Authentication” daily attempt and update timestamp in the TB\_AM\_User table.
	4. Add new logic to detect the “Step-up Authentication” daily attempt count and lock as “Suspect Fraud Lock” if the attempt count is 2 in the table
	5. Add “Suspect Fraud Lock” to user activities table
	6. BVMC Report – update “Fraud Detection” table
	7. Add new dropdown list in BVMC for support centre to change the “Suspect Fraud Lock” to “Fraud Unlock”
2. **Change Limit**
	1. Add logic to store user’s “Change Limit” daily attempt and update timestamp in the IB\_Limit table for all types of limit
	2. Add logic in KFH Online to detect if the change limit by transaction type, if user perform an open or newly added favourite transaction related to the same transaction type (today), the account will be lock as “Suspected Fraud Lock”
	3. Add logic in KFH Online to detect if the change limit is on the “Global Limit”. If user perform any open transaction or newly added favourite transaction (today), the account will be lock as “Suspected Fraud Lock”
	4. Add the “Suspected Fraud Lock” activities to user activities table
	5. Add timestamps column for each limit type in database, estimated 21 types, to keep track of each limit types timestamp

**Impacted System:**

1. KFH Online
2. BVMC
3. CORUS
4. Report
5. Database Table