Minimum Verification Controls

(Version 1.0 - September 2021)

البنك المركزي السعودي
SAMA
Saudi Central Bank

Contents

1. Introduction

While digital innovation is creating major opportunities for the businesses and consumers, at the same time it is also presenting new dimension of emerging threats and changing the traditional view of the cyber risk. To enable member organizations regulated by SAMA to effectively identify and address cyber risks, in addition to the SAMA regulations, SAMA defined a set of controls that must be adopted and implemented by the member organization in order to maintain adequate protection of information assets and digital services.

2. Statement of Applicability

The controls mentioned in this document applies to any member organization that provide E-wallet, lending products, crowdfunding or other fintech business model under SAMA supervision taking into consideration the applicability of the requirements meeting the required objectives.

3. Registration/Onboarding Controls

3.1. Member Organization should ensure registration for each phone number (or) National ID/Iqama, is linked to one application only.

3.2. Member Organization should establish a secure process to validate users.

3.3. The registration process should include the following:

- **a.** For lending platforms: Strong form of authentication from an independent trusted party[1].
- **b.** For E-wallet platforms: Strong form of authentication from an independent trusted party i.e. (National Single

[1] Trusted party: Any party licensed to perform the activity in question

Sign-On (NSSO)) by using user name, password, and OTP.

c. For other business model, robust controls should be implemented in the registration/onboarding process taking into considerations the concept mentioned in points (3.3.a-b).

3.4. Member Organization should verify that the ownership of the phone number is registered to the same user (i.e. match name & national ID) through trusted party only (i.e. Tahaqaq).

3.5. Member Organization should ensure the registration process includes one-time-password mechanism (OTP) as a form of verification. The (OTP) must be send to a verified phone number as per point (3.4).

3.6. Member organizations should implement session timeout controls for all issued (OTP)s.

3.7. SMS notification should be sent to the users for registration, device re-registration or change in the status of account such as deactivation, reactivation and inactive.

3.8. Member Organization application should be assigned to one-device only. Otherwise, an (OTP) should be implemented for each login, as well as disabling concurrent login.

3.9. Member Organization should develop effective and secure process for account deactivation, reactivation and device re-registration to authenticate the user.

4. General Controls

4.1. Member organization should implement regulatory SAMA cybersecurity requirements.

4.2. Member Organization should use official application stores.

4.3. Member Organization should develop installation restriction mechanism for privilege escalation devices such as “Jailbreak” for iOS and “Root” for Android or any open source operating system, taking into consideration that the application is installed through official stores..

4.4. Member organization should have contingency measures in case of disaster and ensure effective back-up and recovery procedures.

4.5. Terms & Conditions should cover data privacy taking into consideration customer consent to display name of account owner.

4.6. Member Organization should conduct awareness program to all users on regular basis that should cover Terms & Conditions and general security awareness such as sharing confidential information (password or OTP).

4.7. Member Organization should develop inactive accounts policy.

4.8. Multi Factor Authentication (MFA) should be implemented to authenticate each log in.

4.9. One-time-password mechanism (OTP) should be implemented for the following processes:

- **a.** Transfer between wallet to wallet (for the first time as minimum for each beneficiary) below (Defined Value)[2];
- **b.** Making any application marketplace transaction;
- **c.** Payment of bills, utility and government services (for the first time as minimum for each bills);
- **d.** Password reset;
- **e.** Wallets reactivations;
- **f.** Risky transactions based on company assessment and use cases.

4.10. One Time Password in one channel and using different delivery channel should be used for following transactions:

- **a.** Any transaction between wallets exceeding (Defined Value) as a daily limit (for first time as minimum for each beneficiary)
- **b.** transfer to IBAN (for first time as minimum for each beneficiary)
- **c.** international transfer (for first time as minimum for each beneficiary)
- **d.** high risk transactions based on company assessment and use cases

[2] Defined value will be circulated in the memo. The value will be reviewed periodically and officially communicated if changed.

4.11. SMS notification should be sent to users for all transactions and user account changes.

4.12. Member Organization should consider the use of comprehensive use cases and scenarios tailored for their business model to combat fraud; including but not limited to:

- **a.** Monitoring the behavior of all users to detect any anomalies based on best practices;
- **b.** Managing device usage behavior;

4.13. Member Organization should establish process to handle fraud cases taking into the consideration investigation and deactivation accounts steps.

4.14. Member Organization should develop a process to safeguard "Data Privacy" and "Data Security" of these accounts. Such information includes "Displaying name of account owner".

4.15. Member Organization should ensure the content of the SMS messages is clear, direct, stating the purpose for the SMS and the name of the Member Organization

4.16. Member Organizations should reflect all controls within this document within their board approved internal policies in their respective organizations, and should have a process in place for periodic review of the polices.

5. Lending Application Special Controls:

The controls below should be implemented by lending companies in addition to the above mention controls.

5.1. Member Organization should have process implemented to assure the recipient IBAN belongs to the loan requester.

5.2. Member Organization should use a trusted and authorized digital signature provider.(see appendix A for additional details)

5.3. Ensure a process is implemented to securely create, save and manage promissory note by using national trusted party (e.g. Nafith)

5.4. Member Organization should implement a process to call the customer to confirm the loan request.

5.5. SMS notification should be sent with customer when:

a. User submitted the request.

b. When the loan request is approved or denied.

6. Appendix A - Overview previous issued SAMA circulars

This document Supersedes the following previously issued SAMA circulars:

- E-Wallet Security Controls v1.0

This document refers to the following SAMA circulars or documents which is mandated as per issued memo:

- Regarding Digital signature for products of Finance companies , 42011675, 1442/02/27;