SECURITY CHECKLIST ON MOBILE APP COLLABORATION

1. Does your app store PII (Personally Identifiable Information) or other sensitive data on the user device?

2. Does your app limit permissions to only the most necessary components required for the app to function correctly?

3. Does your app implement proper TLS by ensuring HTTPS is always used?

4. Does your app hard-code data within the app?

5. Does your app invalidate a user's session upon logout – on both the client and server side? Additionally, does he log users out after a certain amount of inactive time in?
6. Does your app implement OAuth 2.0 where possible to reduce the chance of attackers performing man-in-the-middle attacks?

7. What regulations does your application adhere to (PCI-DSS, HIPAA, etc.)?

8. What platform is your app developed for (IOS, Windows, Android, etc.)?

9. Does your app ensure proper session management (Authentication and Authorization)?

10. Does your app use proper binary protection to combat buffer overflow and stack overflow attacks, along with jailbreaking?

11. What data does your app collects and how are those data secured?

12. Does your app have Non Reverse engineering capabilities?
    This should include the inability to analyse by an unauthorized third party, the final core binary in order not to provide access to the App source code, libraries, algorithms, and other assets.

I/We, on behalf of …………………………………………………..hereby certify that the information provided on this form is accurate. I/We agree that Zenith Bank Ghana Limited reserves the right to take appropriate measures including legal actions if the information here is found to be false.

_________________________ _________________________ _________________
(AUTHORISED SIGNATORY NAME) (SIGNATURE) (DATE)

_________________________ _________________________ _________________
(AUTHORISED SIGNATORY NAME) (SIGNATURE) (DATE)

_________________________ _________________________ _________________
(AUTHORISED SIGNATORY NAME) (SIGNATURE) (DATE)