Privacy Notice

The Hongkong and Shanghai Banking Corporation Limited ('HSBC') collects, uses and shares information about you so that it can provide you with a bank account and related services. This App Privacy Notice explains how HSBC collects, uses and shares your information when you use this app, including information about the device that the app is installed on e.g. your mobile phone or tablet. For full details of our privacy notice, you can find it in our website: https://www.privatebanking.hsbc.com/privacy-notice/privacy-notice-for-the-hongkong-and-shanghai-banking-corporation-limited/.

This app is provided by The Hongkong and Shanghai Banking Corporation Ltd. for iOS version and Android version, and all products and services accessed via this app are provided by HSBC.

You can contact our Data Protection Officer (DPO) and exercise your rights by writing to Level 13 and 14, 1 Queen's Road Central Hong Kong, or contacting us at +852 2899 8777, and marking your letter for the attention of the Data Protection Officer.

We try to protect your personal data against unauthorised or accidental access or processing by using a range of measures, which may include encryption and other forms of security.

We'll take all practicable steps to ensure that your information will not be kept longer than necessary and in line with our data retention policy. We may need to keep your information where we need the information to comply with regulatory or legal requirements, help detect or prevent fraud and financial crime, answer requests from regulators etc. If we no longer need to keep your information, we will destroy or delete it.

This table explains what information HSBC collects from your device and how it uses it. In some cases, e.g. when accessing the contacts stored on your device, or photos that you take with your device, HSBC will first ask your permission. HSBC may share your information with other HSBC group companies, third parties who help us to provide services to you or who act for us or third parties who you consent to us sharing your data with and as explained in our privacy notice.

Permissions for Android devices:

Permission	Used for
Internet connection	Allows applications to connect to the internet.
Internet connection check	Allows us to check if you have a working internet connection.
Device state	Allows us to know if you are on a call while using the app. This helps us to detect and prevent fraud.
Device storage check	Allows the app to save files onto your device's external storage.
Device storage	Allows the app to save and send files from your device's external storage.
Biometric recognition	Allows an app to use biometric recognition for your authentication. If you do so, we rely on your device's technology to authenticate you and we do not collect or store your underlying biometric data.
Wifi connection	Allows us check if you have a working internet connection.
Communication	Allows Samsung devices to support Firebase Cloud Messaging (FCM) feature (see "Cookies" section).
Communication	Migrated from Google FCM. Create an instant-enabled app bundle | Android Developers
Prevent phone from sleeping	Required by older versions of Google Play services to create Firebase Instance ID tokens. These tokens allow us to send notifications to customers.
Notification	Allows an app to popup notifications
Google firebase advertising ID	Allows an app to get the Google firebase Advertising ID, Google push feature will depend on this

Permissions for Apple devices:

Permission	Used for
Camera access	Allows our app to use facial recognition for your authentication.
Facial recognition	Allows our app to use facial recognition for your authentication. If you do so, we rely on your device's technology to authenticate you and we do not collect or store your underlying biometric data.
Location	Allows our app to access your location to help us detect and prevent fraud.

Cookies:
We use the following tools to collect information about your device and the way you use it online.

- AppDynamics – Allows us to track app performance so that it can keep running smoothly
- FCM & Apple Push Notification Service – Allows us to receive push notifications from our servers, related to customer communication
- Google Play Service – Allows us to recognise your approximate location
- RASP – Allows us to detect and prevent malware and fraud, by collecting information about potential risks on your device, for example if it's jailbroken or rooted, or if there are untrusted software keyboards or screen readers installed
- Tealium - Allows us to track your activity within the app to support future enhancements
- Transmit Security – Allows us to secure your login and authentication
- BrightCove – Allows us to track the performance and usage of videos