

Privacy Notice

HSBC is committed to protecting your privacy when you use HSBC Mobile Services. This U.S. Mobile Application Privacy Statement ("Statement") explains how we collect, use, share, and safeguard your information when you use our Mobile Services.

HSBC = HSBC Bank USA, N.A., its banking and non-banking U.S. affiliates and subsidiaries and service providers (collectively, "HSBC USA", "we", "our")

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). You can find full information in our main privacy notice [here](#).

You can contact our Customer Service Center [here](#).

We use a range of measures to keep your information safe and secure which may include encryption and other forms of security. We require our staff and any third parties who carry out any work on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

We'll keep your information in line with our data retention policy. For example, we'll normally keep your main banking information for a period of seven years from when our relationship with you ends. This allows us to comply with legal and regulatory requirements or use it where we need to for our legitimate purposes such as managing your account and dealing with any disputes or concerns that may arise. We may need to keep your information for longer 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 don't need to keep information for this length of time, we may destroy, delete, or anonymise it sooner.

This table explains what information HSBC collects from your device, how it uses it, and whether it shares 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 and any sub-contractors, agents or service providers who work for us or other HSBC group companies (including their employees, sub-contractors, service providers, directors, and officers) to provide you with products or services that you ask for (such as bank accounts and payments) and as explained in our main privacy notice - this type of data sharing is not included in the table.

Permissions for Android devices:

Permission	Used for
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	This allows the app to save and send files from your device's external storage.
Device storage check	This allows the app to save files onto your device's external storage.
Internet connection	Allows applications to connect to the internet
Internet connection check	This allows us to check if you have a working internet connection.
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	This 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 depends 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:

Our app includes tools that collect information about your device and the way you use it online to:

- allow us to track app performance so that it can keep running smoothly
- recognize your approximate location
- 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
- track your activity within the app to support future enhancements
- secure your login and authentication
- track the performance and usage of videos

Some of these tools are provided to us by external service providers and third parties. You can find more information about these in our Online Privacy Statement.