

End User License Agreement

Please read all of this Agreement carefully before downloading and/or using this App.

This Mobile Application ("**App**") is provided by Hang Seng Bank Limited ("**Hang Seng**", "**Bank**", "**we**" or "**us**", which includes our successors and assigns). This End User License Agreement ("**Agreement**") is an agreement between you as the user of the App and the Bank and applies to your use of the App and related technology provided by the Bank. For the avoidance of doubt, this Agreement supplements and shall be read and construed in conjunction with Hang Seng Personal e-Banking Terms and Conditions ("e-Banking Terms and Conditions"), Account Rules, Integrated Account Terms and Conditions, and any other applicable agreements or terms and conditions governing the accounts, services and products provided by us, as may be amended from time to time (together "**Other Terms**").

By clicking "I accept" and downloading the App, you agree to (i) the following terms of this Agreement; and (ii) the **Important Notice** and our **Notice to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance** which are incorporated into this Agreement by reference. All services and features provided via the App shall form part of the "Services" as defined under the e-Banking Terms and Conditions.

1. Data charges (including roaming charges) imposed by your mobile service provider may apply. You are responsible for these charges.
2. You must not use the App on any mobile device or operating system that has been modified outside the mobile device or operating system vendor-supported or vendor-warranted configurations. This includes mobile devices that have been "jail-broken" or "rooted". For the purpose of this Agreement, a jail-broken or rooted mobile device means one that has been freed from the limitations imposed on it by your mobile service provider and the mobile device manufacturer without their approval.
3. Licensed rights and restrictions
 - 3.1. In consideration of you agreeing to abide by the terms of this Agreement, we grant you a non-transferable, non-exclusive license to download and use the App on your mobile device for your personal purposes only.
 - 3.2. You may not use the App for any purpose which is unlawful, abusive, libelous, obscene, threatening or inappropriate in any other way.
4. Trademarks and copyright
 - 4.1. All trade marks, logos and service marks in the App (including but not limited to "HANG SENG" and "恒生" trade marks) are owned by the Bank and other trade mark owners and you are prohibited from using them without our prior written consent.
 - Android, Google Play and the Google Play logo are trademarks of Google LLC.

- Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the US and other countries. App Store is a service mark of Apple Inc.

4.2. All contents in the App (including any text, graphics, links and sounds) are protected by copyright. You are prohibited from modifying, reproducing, storing in a retrieval system, transmitting (in any form or by any means), copying, distributing, re-using, re-posting, reverse-engineering, decompiling, using for creating derivative works or in any other way for commercial or public purposes any part of such contents and related materials without our prior written consent.

5. Disclaimer

5.1. While care has been taken in preparing the information and materials contained in the App, such information and materials are provided to you on an "as is" or "as available" basis. We do not give any warranty or representation of any kind, whether express or implied. In particular, we do not give any warranty or representation regarding non-infringement, security, accuracy, fitness for a particular purpose or freedom from computer virus, Trojan horses, worms, software bombs or similar items ("**Disabling Codes**") in relation to the App or any of the information and materials contained in the App. You are solely responsible for ensuring adequate protection and back up of data and/or equipment for your mobile device, including taking reasonable and appropriate precautions. We are not responsible for any loss, damage or expenses of any kind which you may incur or suffer as a result of or in connection with any of the matters set out in this clause.

5.2. Information (including your Personal e-Banking username and password) sent over the Internet cannot be guaranteed to be completely secure. We are not responsible for any loss, damage or expenses of any kind which you may incur or suffer as a result of or in connection with any delay, loss, diversion, interception, alteration or corruption of any message sent to or received from the Bank at your request, over the Internet. We are not responsible in any manner for any direct, indirect, special or consequential damages which you may incur or suffer arising from or in connection with the use of the App.

5.3. Communication over the Internet may be subject to interruption, transmission blackout, delayed transmission due to Internet traffic or incorrect data transmission due to the public nature of the Internet or any other reason.

6. Third party websites or resources

6.1. The App may offer access to general financial and market information, news services, market analysis, product information and marketing materials prepared and/or issued by persons other than the Bank (together, "**Third Party Information**") and may provide reports compiled from Third Party Information in any form, medium or means. The Third Party Information may be provided in the App or accessible via hyperlinks in the App to third party websites or resources ("**Third Party Websites**"). The contents, accuracy, completeness, timeliness, opinions or views expressed, and other links provided via the Third Party Information or at these Third Party Websites are not investigated, verified, monitored, or

endorsed by the Bank. The Bank expressly disclaims any responsibility for the contents, their availability or errors or omission of Third Party Information found on the App or any of the Third Party Websites that link to or from the App.

- 6.2. You are solely responsible for making all enquiries and investigation before proceeding with any online or offline access or dealing with any person through the Third Party Websites. You understand and accept that all activities conducted by you via or in the App are at your own risk. We do not warrant the security of any information that you may forward or provide to any person via the Third Party Websites. You irrevocably waive any claim against the Bank for any loss, damage or expenses which you may incur or suffer arising from or in connection with any access to or interaction with any of the Third Party Websites via the App.
- 6.3. Hyperlinks to other Hang Seng Bank Group websites or mobile applications ("**Group Websites and Applications**") may be included in the App for your convenience. The products and services offered on the Group Websites and Applications may be limited to persons located or residing in a specified jurisdiction. In addition, the contents on the Group Websites and Applications may not be intended for persons located or residing in any jurisdiction that prohibits or restricts the distribution of such contents. The terms and conditions governing the use of the Group Websites and Applications offered by each Hang Seng Bank Group entity may differ. You should carefully read the terms and conditions applicable to each of the Group Websites and Applications before using or downloading them.

7. Your responsibilities

- 7.1. You are responsible for all claims, damages, liabilities, fees, charges, costs and expenses of any kind arising from:
- 7.1.1. your use of the App;
 - 7.1.2. our reliance on the information provided by you for providing the App; and
 - 7.1.3. any breach by you of this Agreement, any intellectual property or other right of the Bank or any other person.
- 7.2. You are responsible for preventing, safeguarding and ensuring that no Disabling Code is uploaded, transmitted or installed onto or via the App.

8. Termination

- 8.1. We have the right to terminate this Agreement immediately without giving you notice or reason if:
- 8.1.1. you have seriously or persistently breached any of the terms of this Agreement;
 - 8.1.2. we know or reasonably suspect you have committed or are about to commit fraud or any other illegal or improper act in connection with your bank account (including non-compliance with any requirements relating to anti-money laundering, counter-terrorist

financing, sanction regime or tax regime);

8.1.3. you are not eligible or entitled to download the App for any reason; or

8.1.4. if the App is withdrawn by Apple or, Google Inc. for any reason.

8.2. You may terminate this Agreement at any time by deleting the App from your mobile device.

9. Governing law and jurisdiction

9.1. This Agreement is governed by and shall be construed in accordance with the laws of the HKSAR.

9.2. You submit to the non-exclusive jurisdiction of the courts of the HKSAR.

9.3. This Agreement may be enforced in the courts of any competent jurisdiction.

10. Governing version and variation of this Agreement

10.1. The English version of this Agreement shall prevail to the extent of any inconsistency between the English version and the Chinese version.

10.2. We have the right to vary the provisions of this Agreement and/or the Important Notice and/or our Notice to Customers and Other Individuals relating to the Personal Data (Privacy) Ordinance from time to time and notify you of the variations when you next launch the App. You are required to read and accept the variations before continuing your use of the App. If you do not accept the variations, you should cease to use the App.

11. Mobile Security Key and Biometric Authentication

Definitions

11.1. "Biometric Authentication" means the identity authentication function using biometric credentials (including fingerprint, iris, facial map or any other biometric data), as we may provide from time to time pursuant to this Agreement.

11.2. "Mobile Security Key" means a feature within the App which is a software-based Security Device used to generate a one-time Security Code, as we may provide from time to time pursuant to this Agreement.

11.3. "Permitted Mobile Device(s)" means such as Apple device and compatible Android device running an operating system version as we specify from time to time, or any other electronic devices or equipment which we may enable for using Mobile Security Key or Biometric Authentication from time to time.

Mobile Security Key

11.4. Mobile Security Key provides an alternative means of verifying your identity for accessing the Services. You may register the Mobile Security Key on your Permitted Mobile Device(s) by completing the steps specified by us.

- 11.5. Once successfully registered, you have to use the password associated with the Mobile Security Key on your Permitted Mobile Device(s) to confirm your identity for accessing the Services.
- 11.6. You may also use Mobile Security Key to generate a one-time Security Code as a second verification when performing certain Personal e-Banking transactions which require the Security Code.
 - 11.6.1. You may use Mobile Security Key to verify your identity and instructions via the App for services or transactions (not limited to Personal e-Banking and App transactions) which the Bank may specify from time to time.
- 11.7. You may deactivate Mobile Security Key at any time via the App by completing the steps specified by us. Once deactivated, you may not be able to continue to access the Services if Mobile Security Key is deemed necessary for accessing the services.
- 11.8. We have the right to specify or vary from time to time the scope and features of Mobile Security Key without prior notice.
- 11.9. You can set up Mobile Security Key on one or multiple (if applicable) Permitted Mobile Device(s) which we will identify by way of your mobile device ID.

Biometric Authentication

- 11.10. Biometric Authentication provides an alternative to using your Mobile Security Key password to verify your identity for accessing the Services. You have to register your Permitted Mobile Device(s) (with biometric identity sensor supported) for Biometric Authentication by completing the steps specified by us.
- 11.11. Once successfully registered, you may use your biometric credentials registered on the Permitted Mobile Device(s) to: confirm your identity for accessing the Services via the App; and to generate a one-time Security Code as a second verification when performing certain Personal e-Banking transactions which require the Security Code.
 - 11.11.1. You may also use Biometric Authentication to verify your identity and instructions via the App for services or transactions (not limited to Personal e-Banking and App transactions) which the Bank may specify from time to time.
- 11.12. Having registered for Biometric Authentication, you may still choose to access the Services by using your Mobile Security Key password.
- 11.13. You may deactivate Biometric Authentication at any time by completing the steps specified by us. Once deactivated, you may continue to access the Services by using your Mobile Security Key password.
- 11.14. We have the right to specify or vary from time to time the scope and features of Biometric Authentication without prior notice.

Rights and Responsibilities

- 11.15. By registering the Mobile Security Key and/or Biometric Authentication, you authorise us to (a) verify your identity by any Mobile Security Key or biometric credentials registered on your Permitted Mobile Device(s), (b) verify your identity by the Mobile Security Key or biometric credentials registered on your Permitted Mobile Device(s) as a second verification for logging on to Hang Seng Personal e-Banking or performing Personal e-Banking transactions which require a one-time Security Code, and/or (c) verify your instructions for services or transactions (not limited to Personal e-Banking and App transactions) which the Bank may specify from time to time by any Mobile Security Key or biometric credentials registered on your Permitted Mobile Device(s), as if each Mobile Security Key or biometric credential were a username, password, PIN, identifier, Security Code or other security code for identifying you or verifying your instructions for the purposes of accessing accounts, services or products under the Other Terms.
- 11.16. In order to use Mobile Security Key or Biometric Authentication:
- 11.16.1. you must be a valid user of the Services;
 - 11.16.2. you must install the App using your Permitted Mobile Device(s);
 - 11.16.3. you must register a password for the Mobile Security Key on your Permitted Mobile Device(s); and
 - 11.16.4. (for Biometric Authentication) you must activate the biometric identity sensor on the Permitted Mobile Device(s) and register at least one of your biometric credentials to control access to the Permitted Mobile Device(s).
- 11.17. You fully understand and agree that:
- 11.17.1. upon successful registration for Biometric Authentication, ALL biometric credentials stored on the Permitted Mobile Device(s) registered for Biometric Authentication at the time of or after registration can be used to access the Services or give instructions for other services or transactions. Therefore, you must ensure that only your own biometric credential is stored on the Permitted Mobile Device(s). If you store any other person's biometric credential or allow any other person's biometric credential to be stored on the Permitted Mobile Device(s), you are responsible for any person using the other biometric credential to access the Services or give instructions for other services or transactions, including operating your accounts and effecting transactions. All such dealings and transactions will be deemed to be authorised by you and will be binding on you;
 - 11.17.2. each time the App detects the use of biometric credentials registered on the Permitted Mobile Device(s) registered for Biometric Authentication to access the Services, you are deemed to have accessed the Services; and
 - 11.17.3. the authentication is performed by the App by interfacing with the biometric identity sensor module on your Permitted Mobile Device(s). We do not collect your biometric

credentials. The App will access the biometric identity sensor in your Permitted Mobile Device(s) and obtain the necessary information to perform the authentication. You consent to the authentication process and our accessing and using the information obtained via the biometric identity sensor.

11.18. You should take all reasonable security measures to prevent unauthorised or fraudulent use of Mobile Security Key or Biometric Authentication, including the following measures:

11.18.1. you should take reasonable precautions to keep safe and prevent loss or fraudulent use of your Permitted Mobile Device(s), Hang Seng Personal e-Banking username and password, and the Mobile Security Key password. You should observe the security recommendations provided by us from time to time about the use of Mobile Security Key or Biometric Authentication;

11.18.2. you must not use the App, Mobile Security Key or Biometric Authentication on any mobile device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations. This includes devices that have been "jail-broken" or "rooted". A jail-broken or rooted device means one that has been freed from the limitations imposed on it by your mobile service provider and the phone manufacturer without their approval. The use of the App, Mobile Security Key or Biometric Authentication on a jail-broken or rooted device may compromise security and lead to fraudulent transactions. Download and use of the App, Mobile Security Key or Biometric Authentication in a jail-broken or rooted device is entirely at your own risk and we will not be liable for any losses or any other consequences suffered or incurred by you as a result;

11.18.3. you should not use facial recognition for Biometric Authentication if you have an identical twin sibling;

11.18.4. you should not use facial recognition for Biometric Authentication if you are an adolescent while your facial features may be undergoing a rapid stage of development

11.18.5. you should not take any action to disable any function provided by, and/or agreeing to any settings of, your mobile device(s) that would otherwise compromise the security of the use of your biometric credentials for Biometric Authentication (e.g. disabling "attention-aware" for facial recognition); and

11.18.6. if you are aware of or suspect any unauthorised use of your Permitted Mobile Device(s) or Hang Seng Personal e-Banking username and password or Mobile Security Key password for effecting Mobile Security Key or Biometric Authentication, you should notify us as soon as reasonably practicable by calling our 24-hour Customer Service Hotline at 2822 0228. We may require you to change your Hang Seng Personal e-Banking username and password, re-register Mobile Security Key, re-register your biometric credentials or cease to use Mobile Security Key or Biometric Authentication.

11.19. All instructions received by us with your identity verified through the Mobile Security Key or Biometric Authentication shall be binding on you. You are liable for such instructions and all

resulting transactions in accordance with the provisions of the Other Terms, including the provisions relating to your liability for unauthorised transactions if you acted fraudulently or with gross negligence.

- 11.20. We have the right to modify, suspend or terminate Mobile Security Key and/or Biometric Authentication or its/their use by you at any time without giving prior notice or reason where we reasonably consider necessary or advisable to do so. These cases may include actual or suspected breach of security.

Limitation of our Liability

- 11.21. Mobile Security Key or Biometric Authentication is provided on an "as is" and "as available" basis. We do not warrant that Mobile Security Key or Biometric Authentication will be available at all times, or that it will function with any electronic equipment, software, system or other Services that we may offer from time to time.
- 11.22. The biometric identity sensor module on your Permitted Mobile Device(s) is not provided by us. We are not responsible for the biometric identity sensor technology.
- 11.23. We are not liable for any loss, damages or expenses of any kind incurred or suffered by you arising from or in connection with your use of or inability to use Mobile Security Key or Biometric Authentication unless it is caused solely and directly by the negligence or willful default on our part or on the part of our employees or agents.
- 11.24. Under no circumstances are we liable for any indirect, special, incidental, consequential, punitive or exemplary loss or damages, including loss of profits, loss due to business interruption or loss of any programme or data in your Permitted Mobile Device(s).

Important Notice, Disclaimer and Risk Warning

Important Notice

By accessing this App you are agreeing to the terms set out below and by continuing to use this App following the posting of any changes to these terms will signify your consent to the changes made.

Cross Border Disclaimer

This App is provided by Hang Seng Bank Limited ("the Bank" or "we"). The Bank is regulated and authorised to carry out banking activities in Hong Kong SAR. The products and services represented within this App are intended for Hong Kong customers.

This App is not intended for distribution, download or use by any person in any jurisdiction, country or region where the distribution, download or use of this material is restricted and would not be permitted by law or regulation. If you are outside of Hong Kong, we may not be authorised to offer or provide you with the products and services available through this App in the country or region you are located or resident in.

General

Hang Seng of 83 Des Voeux Road, Central, Hong Kong is incorporated in Hong Kong with limited liability.

The information contained in this App is not and is not intended to provide investment or other professional advice. Persons downloading or using this App should obtain advice from their own professional adviser as appropriate.

The Bank has discretion whether or not to provide any information, products or services described in this App to any person. Any information, products or services described in this App may be withdrawn or amended at any time without advance notice at the discretion of the Bank.

Security reminder

The Bank maintains strict security standards and procedures to prevent unauthorised access to information about you. The Bank will never contact you by email or other means and ask you to provide or validate your personal information such as your user ID, account number or password. If you receive such a request, you should contact the Bank at (852) 2822 0228. Please communicate with the Bank through our official website domain address (www.hangseng.com) and not through any hyperlink embedded in any e-mail.

Please also refer to our [security reminders](#) which may be updated from time to time.

Our Data Privacy Principles

In this Privacy Policy, “Hang Seng”, “we”, “us” or “our” means the Hang Seng Bank Limited.

We have built our business on trust between our customers and ourselves. To preserve the confidentiality of all your personal data shared with us, we adopted our Data Privacy Principles. By maintaining our commitment to these Data Privacy Principles, we will ensure that we respect the trust you place in us.

1. Transparency

We will:

- be clear and transparent about how we collect and use data; and
- give data subjects any required statements on how we may use their data. Data subjects include personal customers, corporate customers, representatives and non-affiliated third parties (such as vendors and their representatives).

2. Fair and lawful usage

We will only collect, process and store data:

- lawfully; and
- if we have a legitimate reason.

3. Limited purposes

We will:

- collect and process data for specific and lawful purposes; and
- not use it for other purposes unless we take all steps required under any data privacy laws and regulations which apply.

4. **Data minimisation and adequacy**

When we collect, retain and process data, we will strike an appropriate balance between:

- processing sufficient data to carry on our business and achieve any specified lawful purposes; and
- ensuring that we do not collect, retain or process excessive amounts of data.

5. **Data quality and accuracy**

We will:

- maintain appropriate standards of data quality and integrity; and
- implement policies for data accuracy. This includes taking steps to avoid data becoming out of date where appropriate.

6. **Privacy by Design**

We ensure:

- that new products and services, or changes to existing products or services, are designed to respect data privacy laws; and
- every individual who works with personal data is aware of their legal obligations and their responsibility to follow these principles.

7. **Data security and retention**

We will:

- retain data securely, implement appropriate data retention policies, and dispose data securely once it is no longer required; and
- ensure that we will only authorise those with a legitimate justification to access such data.

8. **Training and awareness**

We will ensure our employees are properly trained on their obligations for processing your data.

9. **Data subject rights**

We will ensure that data subjects' rights are observed as set out in applicable data privacy laws and regulations.

10. **Third parties**

We will require any vendor or agent to apply standards equivalent to these Data Privacy Principles. We will only disclose data to:

- governmental or judicial bodies;
- law enforcement agencies; or
- our regulators,

where this is allowed by any laws and regulations which may apply.

11. **Data transfers**

Sometimes we may transfer data to another HSBC Group entity and/or third party (local and/or overseas). We will

- ensure such data transfer is lawful; and
- assure the recipient applies the same, or equivalent, standards as these Data Privacy Principles.

We will, at all times, observe the Personal Data (Privacy) Ordinance ("the Ordinance") of the Hong Kong SAR in collecting, maintaining and using the personal data of customers as per the [Privacy Notice](#).

Contact Us

You can ask us for:

- access to your personal data or correction of your personal data; or
- information regarding policies and practices on personal data and the kinds of personal data held.

You will need to address your request to:

Data Protection Officer
Hang Seng Bank Limited
83 Des Voeux Road Central
Hong Kong SAR
Fax : (852) 2868 4042

Marketing Promotions

We collect your personal data

We only collect personal data from you if you agree to share it with us. Occasionally, we may collect personal data from you when you:

- visit this site or our mobile application; or
- when you give us your consent in other connections (e.g. when you participate in a contest or promotion).

The [Privacy Notice](#) governs the collection and use of your personal data.

We may use your personal data:

- to inform you of products, services and other marketing materials. We usually do this if we think they may be of interest to you;
- to invite you to take part in market research, surveys and other similar activities via us or our external research agencies; and
- for direct marketing

You can find more details in the direct marketing section of the [Privacy Notice](#).

You can opt out of our marketing

You can choose to receive marketing and other promotional materials by post, SMS, MMS, phone, email or push notification. You may opt out at any time. You can tell us if you wish to opt out via our branches, customer service hotline, e-Banking or mail. Marketing push notifications can only be

turned off via mobile application.

You can ask us to stop sending you direct marketing promotions by calling:

- (852) 2998 8022 for Prestige Private Banking customers
- (852) 2998 9188 for Prestige Banking customers
- (852) 2822 8228 for Preferred Banking customers
- (852) 2822 0228 for other customers

We will take action on your request within 30 days at no cost to you.

Use of Big Data & Artificial Intelligence ("BDAI")

BDAI enables companies to process and analyse data at a scale. This has never been possible before. We are using big data and AI to:

- bring benefits to our customers, for example, by improving customer service;
- manage risks for ourselves and our customers;
- better identify and offer relevant products and services to customers; and
- improve operational efficiencies.

Using BDAI brings new responsibilities. We must ensure that BDAI is used ethically. We have a set of principles to help us do this. You can find our Principles for the Ethical Use of Data and Artificial Intelligence [here](#).

Push Notification

We may send you push notifications based on your preference made on the settings of this App. Your preference will be captured by this App and sent to the Bank for the purpose of sending (and in which language) or not sending you push notifications.

Use of cookies

This Cookies Policy is for Hang Seng Bank Limited (this "Policy"). In this document, "Hang Seng", "we" or "us" means Hang Seng Bank Limited (including any successors and assigns).

We may gather the following information using cookies.

What are cookies?

Cookies are text files with small pieces of data. They are automatically stored on your browser. Cookies can be read by:

- our website and application; and
- other websites and applications that recognise the cookies.

Cookies can collect information about your behaviour on websites. They are widely used to store and receive identifiers and other information on devices. You can manage your cookies settings at any time.

We may also use other tracking technologies similar to cookies such as pixel tags, and tracking URLs for similar purposes. This includes collecting data stored on your web browser or device and identifiers associated with your device and other software. In this policy we refer to all of these technologies as “cookies”.

You can change or turn off cookies

Most browsers are initially set to allow cookies. You can turn off cookies through your browser settings. Your browser's "Help" function should tell you how to do this. If you turn off cookies, you may not be able to fully use our website and application. For example, you will not be able to log on and use Hang Seng e-Banking services.

You acknowledge that your information and personal data (if any) are being collected, stored, accessed and used as set out in this Cookies Policy while using our website or application unless you have turned off cookies.

How we use cookies

We use cookies to:	So we can:
Record your visit to our website or application.	Analyse the number of visitors and users' general usage patterns. We use this data to help improve our products and services.
Record your personal use habits, profiles, preferences and interests based on your use of our website or application.	Improve your experience with our website and application.
Recognise your device and store information about your: <ul style="list-style-type: none">personalised settings (e.g. language preference and useful links settings); anduse of our website or application. This includes visit and login sessions, your behaviour, such as what you view and click, as well as your pattern and footprints.	Provide you with a more personalised service. We use this data to customise our website content and applications to suit your interests.

We can access the information stored in cookies. This information may be combined and compared with your other personal data collected and used by us as set out in our [Privacy Notice](#). This may include information like:

- demographic data;
- transaction details and transaction patterns; and
- product holdings.

We use this information for analytical, direct marketing, and fraud detection and fraud prevention.

We may also use this data and your personal information to provide you with promotional materials or direct marketing. We will only do this if you have given us consent. You can update your marketing preferences from time to time.

Sharing data with third parties

Third parties (as listed below) may research certain uses and activities on our website or application on our behalf. They use technologies such as:

- tracking tags and cookies;
- spotlight monitoring (e.g. managing tagging, which tracks which advertisement users clicked to take them to the website); and
- web beacons (monitoring the behaviour of the user, such as page scrolling).

Third parties use this information:

- to find out more about users of our website and application. This includes the number of visitors, user demographics, preferences, interests, behaviour and usage patterns;
- for internal reporting; and
- to improve the effectiveness of our marketing.

Our third parties collect information and share it with us. The shared information may be combined and matched with your personal data collected by us (at any time) as set out in our [Privacy Notice](#). This means your identity may be directly or indirectly ascertained. We may share information about you with our third parties. This includes your advertising identifier, "installation event" (which means the data in relation to when you first install or use our website/application) and digital footprint. Personal identifiable information about you may be collected or shared by third-party agencies with us as a result of this research.

To find out more about the use of cookies and the information-collecting practices and opt-out procedures of third-parties research agencies, please visit:

- Appier <https://www.appier.com/en/about/privacy-policy>
- Bing <https://privacy.microsoft.com/en-us/privacystatement>
- Biocatch <https://www.biocatch.com/privacy-policy>
- Brightcove <https://www.brightcove.com/en/legal/cookie-policy/>
- Google Campaign Manager (DoubleClick Campaign Manager)/ Google Display & Video 360 (DoubleClick Bid Manager)/ Google Webmaster's <http://www.google.com/intl/en/policies/privacy/>
- LinkedIn <https://www.linkedin.com/legal/cookie-policy>

- LivePerson LiveEngage 2.0 <https://knowledge.liveperson.com/security-regulations-liveperson-cookies.html/>
- Meta <https://www.facebook.com/privacy/policies/cookies>
- Optimizely <https://www.optimizely.com/legal/privacy-policy/>
- Qualtrics <https://www.qualtrics.com/privacy-statement/>
- Taboola <https://www.taboola.com/policies/privacy-policy>
- Tealium <https://tealium.com/cookie-policy/>
- The Trade Desk <https://www.thetradedesk.com/us/privacy>
- Threatmetrix <https://risk.lexisnexis.com/group/privacy-policy>
- Vpon <https://www.vpon.com/en/privacy-policy/>
- Yahoo <https://legal.yahoo.com/us/en/yahoo/privacy/topics/cookies/index.html>

All of these links are external to Hang Seng Bank. We are not responsible for the content of these links.

Disclaimer

All information and services provided herein are solely for personal and non-commercial use and for general information and reference only. Re-distribution of any part by any means is strictly prohibited. The information provided in this App, including but not limited to general financial and market information, news services and market analysis prepared and/or issued by persons other than the Bank and/ or the Bank (together “**Market Information**”) contained herein does not intend to and should not be regarded as an offer or solicitation or recommendation to buy or sell any investment products. The information contained herein is for general information and reference purposes only and is not intended to provide professional investment or other advice. It is not intended to form the basis of any investment decision. Persons accessing this App should not make any investment decision based solely on the information and services provided herein. Before making any investment decision, persons accessing this App should take into account his/her own circumstances including but not limited to his/her financial situation, investment experience and investment objectives, and should understand the nature, terms and risks of the relevant investment products. Persons accessing this App should obtain appropriate professional advice where necessary. Hang Seng Bank Limited (the “Bank”) does not guarantee the accuracy and reliability of the Third Party Information and Market Information provided herein and accepts no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracies or omission.

Market Information relating to Local Securities

Market Information relating to local securities (including warrants and Callable Bull/Bear Contracts (“CBBC”)) may be provided by BNP Paribas Hong Kong Branch, Credit Suisse (Hong Kong) Limited, ET Net Limited, Hang Seng Indexes Company Limited, Macquarie Capital Securities Limited, SG Securities (HK) Limited, The Hongkong and Shanghai Banking Corporation Limited, The Stock Exchange of Hong Kong Limited, UBS AG London Branch, China Investment Information Services Limited (including its holding companies and/or any subsidiary of such holding companies), Shenzhen Securities Information Company Limited, London Stock Exchange Group

plc and its group undertakings (collectively, the “LSE Group”) (together the “Information Providers”) and the Bank. The Information Providers and the Bank endeavour to ensure the accuracy and reliability of the Market Information provided but do not guarantee its accuracy or reliability and accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracies or omission. For information which is “Powered by” the Information Providers, it is being re-transmitted by the Bank in the ordinary course of business to you for general information and reference purposes only. The Bank, its officers, employees, and agents did not devise, select, add to, modify or otherwise exercise control over its contents, do not take responsibility for it nor do they endorse the accuracy of such information.

Market Information relating to Investment Funds

Market Information relating to investment funds may be provided by Morningstar Asia Limited (the “Information Provider”) and Hang Seng Bank Limited (the “Bank”). The Information Provider and the Bank endeavour to ensure the accuracy and reliability of the Market Information provided but do not guarantee its accuracy or reliability and accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracies or omission. Where the Market Information related to investment funds is sourced externally (as disclosed), the Bank has reasonable belief that such Market Information is accurate, complete and up-to-date. For information which is “Powered By” the Information Provider and other fund houses, it is being re-transmitted by the Bank in the ordinary course of business to you for general information and reference purposes only. The Bank, its officers, employees, and agents did not devise, select, add to, modify or otherwise exercise control over its contents, do not take responsibility for it nor do they endorse the accuracy of such information. This App and the information provided in this App relating to investment funds have not been reviewed by the Securities and Futures Commission in Hong Kong (“SFC”).

Risk Warning

All investments involve risks. Prices of securities, foreign exchange, commodity and investment products may go up or down and may become valueless. Investors should read the relevant risk disclosure statement, offering/product document and terms and conditions in detail before making any investment decision.

Risk of Investing in RMB Securities

Stock Connect Terms

Warrants, CBBC and Inline Warrant

The prices of warrants, CBBC and Inline Warrant can fluctuate dramatically. Warrants and CBBC may expire worthless, resulting in a total loss of investors’ investment. For Inline Warrant, the profit potential is capped by the pre-determined payment. Investors should note that, at times, the issuer of the related warrants, CBBC or Inline warrant may be the only person quoting prices on the exchange. It is as likely that losses be incurred as profits made from buying and selling securities.

CBBC has a mandatory call feature. CBBC must be terminated when the spot price/spot level of the underlying asset reaches or goes beyond the call price/call level prior to expiry, in which case, the holder of CBBC will or is likely to, lose all the investment. Investors bear the credit risk of the issuer and have no recourse to the Bank. Investors should make their own risk assessment and seek independent professional investment or other advice where necessary with respect to any exposure to warrants, CBBC or Inline Warrant. Investors should refer to the relevant risk disclosure statement, offering/product document and terms and conditions before making any investment decision. Trading Inline Warrant below the Minimum Fixed Payment at Expiry or above the Maximum Fixed Payment at Expiry may not reflect the true value of the Inline Warrant. Any inline warrant trades executed at the price above the Maximum Fixed Payment at Expiry will not be recognized and will be cancelled by HKEX.

Exchange Trade Funds (ETFs) (include Leverage and Inverse (L&I) Products)

There is tracking error risk for ETFs. The market price of an ETF may be at a discount or premium to its net asset value. L&I Products are not intended for holding longer than the rebalancing interval, typically one day, it is possible that the leveraged product will lose money over time while the underlying index increases or is flat. There is no assurance that L&I Products can rebalance their portfolios on a daily basis to achieve their investment objectives. Leverage factor of L&I Products may change during a trading day which make its return during a trading day may be greater or less than the leveraged/opposite return of the underlying index.

IPO Stocks

Investors should read the relevant prospectus for detailed information about the proposed offer and seriously consider if investment in the relevant shares is suitable for his/her investment needs by reference to his/her financial situation, investment experience, investment objectives and other conditions and needs before deciding whether to invest in the relevant shares. If required, investors should obtain independent legal, financial and other professional investment or other advice before making any investment decision. The Market Information contained herein does not constitute an offer, an invitation, an inducement, a solicitation or recommendation by the Bank to any person to acquire, purchase or subscribe for the shares proposed to be offered.

Free Real-time basic quote

Free Real-time basic quote is provided for free. Data content includes nominal/last traded price, closing price, today's high/low prices, trading volume, turnover value, Indicative Equilibrium Price (IEP) and Indicative Equilibrium Volume (IEV) during the pre-opening session of individual securities on the Stock Exchange.

Investment Funds

Investors should note that all investments involve risks (including the possibility of loss of the capital invested), prices of fund units may go up as well as down and past performance information presented is not indicative of future performance. Investors should read the relevant fund's offering documents (including the full text of the risk factors stated therein (in particular those associated with investments in emerging markets for funds investing in emerging markets)) in detail before

making any investment decision. The information contained herein is not intended to provide professional investment or other advice. Persons accessing this App should obtain appropriate professional advice where necessary.

Currency Risk

Foreign Exchange involves Exchange Rate Risk. Fluctuations in the exchange rate of a foreign currency may result in gains or losses in the event that the customer converts HKD to foreign currency or vice versa.

RMB Currency Risk

Renminbi ("RMB") is subject to exchange rate risk. Fluctuation in the exchange rate of RMB may result in losses in the event that the customer subsequently converts RMB into another currency (including Hong Kong Dollars). Exchange controls imposed by the relevant authorities may also adversely affect the applicable exchange rate. RMB is currently not freely convertible and conversion of RMB may be subject to certain policy, regulatory requirements and/or restrictions (which are subject to changes from time to time without notice).

The actual conversion arrangement will depend on the policy, regulatory requirements and/or restrictions prevailing at the relevant time.

Note: In case of discrepancies between the English and Chinese version, the English version shall apply and prevail.