



Terms and Conditions for HSBC Online and Mobile Banking

You must read these terms and conditions carefully before using the services.

By registering to use the services, you shall be deemed to have accepted and be bound by all these terms and conditions.

How your Online and Mobile Banking works

How your Online and Mobile Banking works

These terms apply if you use Online or Mobile Banking or any of the services.

When we talk about "we", "our" or "us" in these terms and conditions, we mean HSBC Philippines Limited.

When we talk about "you" or "your" in these terms and conditions, we mean you, our customer or the person who has downloaded or used the Mobile Banking app or Online Banking. Where more than one person is authorised to operate an account, every reference in these terms and conditions to "you" is deemed to include each and all of the account holders and each and all of the persons authorised to operate the account. All of you are jointly and severally liable under these terms.

How we check it's you

To confirm it's you when using Online or Mobile Banking, we'll ask you for security details like a password, security code, biometric data or information you use with your device like a mobile phone number.

If we aren't sure if it's you or we can't verify your identify:

- We might ask further questions
- There might be a delay to your transaction
- We might not be able to process your instructions
- Sometimes we might even have to block your account

We may, in our discretion, decline or delay acting on any instructions as long as we're acting in good faith. The reasons for doing so include if:

- We are verifying your identity or your instructions
- The value of your transaction is higher than any limits we set
- We suspect there's been a breach of security

We won't compensate you if there's a delay or you lose money as a result of our actions to keep your account safe.

We'll act on an instruction if we reasonably believe that it's given or authorised by you. We may do this even if your instructions conflict with any previous instructions you've given us.

Make sure only your biometric data are registered on your device.

Biometric data means things like fingerprints, facial or voice recognition or a retinal image.

Don't use facial recognition if you have an identical twin sibling or if your facial features are undergoing a rapid stage of development (such as during adolescence).

Don't disable any function or settings provided by your device which could compromise your biometric data, for example, disabling Attention Aware features for facial recognition on iOS.

Security Key

We may give you a Security Key to access Online and Mobile Banking. This may be a physical electronic device or Digital Security Key that generates one-time passwords. If your Security Key needs replacing, we may charge you PHP500.

When Online and Mobile Banking might not be available

- If we're undertaking maintenance or upgrades. We do this to make sure our services remain compatible with supported devices, browsers and operating systems. This might mean there are periods of time where the services are unavailable. We'll try to tell you before we do this.
- If we're unable to provide it due to legal, regulatory, technical or other reasons beyond our control

We'll let you know what operating requirements you'll need to access Online or Mobile Banking. If you don't meet these requirements, you may not be able to access Online or Mobile Banking.

Keep your browser, operating system and Mobile Banking app updated to the latest versions to ensure you have access to Online and Mobile Banking. If you're not up to date with the latest upgrades, some of our features and services may not be available.

Please also check your online or mobile service and contact your provider if access issues occur.

As Mobile Banking is an app, it:

- Has different functions compared to Online Banking
- May store some of the information you share or create on the Mobile Banking app on your device

Instructions, getting advice and the information we display

Sometimes we quote exchange, interest or dealing rates or other prices in Online or Mobile Banking. These rates are just for information and the rate or price we confirm at the time of you agreeing to proceed might be different.

Please make sure you verify any data or reports before acting upon them, for example, market prices.

Submit an instruction before the daily cut-off time to avoid waiting until the next banking day for the instruction to be processed.

If you want to change or cancel an instruction, tell us as soon as possible. We may not be able to act on your new instruction if we've already completed or started to carry out your initial instruction.

Please check any transaction confirmation that we send to you immediately and tell us straight away if you notice a mistake. If you transfer money to the wrong person by mistake, we'll do our best to get it back but can't guarantee it.

You must provide any information we reasonably ask for about a transaction.

For products or services sold via Online or Mobile Banking, these are execution only transactions based on your own judgement and you should carefully assess whether these transactions are suitable for you. Any prior recommendation we may have provided to you was suitable at the time it was made. We have no ongoing responsibility to ensure that a product we have recommended to you remains suitable for you.

You may be able to see products or services through Online or Mobile Banking which you may have bought outside of Online or Mobile Banking and that you hold via us, another HSBC Group company or certain third parties.

Using your location

Sometimes Online and Mobile Banking uses information about your location sent from your device.

If you use these location services, you're agreeing to us and sometimes third parties accessing, monitoring, transmitting, collecting, storing, disclosing, processing and using your location data. We'll only collect, use, store and disclose your location data as explained in our privacy notice.

Sometimes if you're using third-party services on your device through Online and Mobile Banking, they have their own terms about how they'll use your data which you need to check and agree to.

We'll ask if you agree to the use of your location data when you first use Online or Mobile Banking.

You can turn off the location services settings on your device at any time if you don't want us or our third-party service providers to access your location information.

Fees

We don't charge for using Online or Mobile Banking, but you may be charged for executing certain actions through it. Details of our fees and charges can be found in our [Bank tariff guide](#), which you can find on our website.

We also won't charge you for the tool / application you need to use to generate a security code to access our Online and Mobile Banking, but the type of tool / application you need to use may change over time as technology evolves.

We may give you a Security Key to access Online and Mobile Banking. This may be a physical electronic device or Digital Security Key that generates one-time passwords. If your Security Key needs replacing, we may charge you PHP500.

We may change these terms including by introducing other charges. If you don't agree with these changes, you can stop using Online and Mobile Banking.

To use Online and Mobile Banking, you'll need an internet connection or mobile phone service plan. You're responsible for any fees and charges for these services.

Where you can use Online and Mobile Banking

We designed Online and Mobile Banking to meet legal and regulatory requirements for our customers physically residing in the Philippines. This means we might not be authorised to offer you the products and services available through Online and Mobile Banking if you move countries or regions. Online and Mobile Banking is not intended for distribution, download or use by any person in any jurisdiction, country or region where this would not be permitted by law or regulation.

Travelling abroad

If you're travelling, the laws and regulations of some countries and regions may prevent us from actioning your requests. For example, the country or region you've travelled to may deem any transfer of money between your investment funds as "trading securities" under their laws and regulations. This can have unintended legal and taxation effects. For this reason, we'll tell you when we reasonably believe that complying with a term or condition would cause us to breach any laws meaning we may decline to honour some or all of your requests. We'll be able to action your requests after you return home.

HSBC kiosks and devices

You can use HSBC Kiosks and any other computing devices or terminals ("HSBC Devices") to access Online Banking. If you do this, you agree:

- You won't use HSBC Devices for anything illegal and you'll comply with all applicable laws
- You'll tell us straight away if you become aware HSBC Devices being used for or in relation to an illegal activity
- You won't use HSBC devices to:
 - Create, access, use or share obscene or objectionable material
 - Share information or software containing electronic worms, viruses or other harmful components
 - Break or attempt to break into computer systems
 - Download, install or store any third-party programs
 - Copy, upload, post, publish, transmit, reproduce or distribute material that's copyright protected without obtaining permission from the copyright owner or rightsholder

While we've tried to ensure HSBC Devices operate properly and are secure, we can't guarantee there are no viruses, spyware or any other malicious computing software on HSBC Devices.

We won't be responsible for any loss you may suffer when using HSBC Devices.

We or our third-party service providers may track your activities on HSBC Devices. This includes your use of your Username or Online Banking ID, Password, Password Reset Questions and Security Codes.

If you breach these terms, we can withdraw your access to HSBC Devices.

Bill payment services

Our bill payment services allow you to pay bills issued by certain merchants. You can pay bills issued to you or others. ("Bill Customers").

You'll need to pay interest, charges and fees to the merchant if you don't pay bills on time.

If you ask us to pay a bill for you, we'll debit your account. You'll need to ensure you have enough money in your account to do this. You may also use your available credit. If we do so, you're responsible for the amount owed. We don't have to tell you before we do this.

Complaints

If you have a disagreement with a merchant or any Bill Customers, you must take it up directly with them. Any disputes with any merchant, bank, financial institution or any other person don't affect our rights under these terms.

Making payments

You can make payments to anyone who's registered their:

- Bank account details or e-wallet with a participating non-financial institution

Payments can be made from any current or savings account held:

- In your sole name
- Jointly with another person (where the signing mandate is for each individual to sign singly)

Web Chat

This would govern the access to and use of Web Chat enabling HSBC agents to interact with HSBC customers and respond to requests about HSBC's products, services and other assistance in relation to your account, application and transactions.

You must only use Web Chat for the purposes described in these terms of Use. You must not use or attempt to use Web Chat to:

- Jeopardise the reputation of HSBC or LivePerson
- Damage or interfere with Web Chat data, software, website or information technology systems
- Send any offensive, provocative, defamatory, fraudulent or otherwise unlawful information or communication on Web Chat
- Cause annoyance or inconvenience to HSBC or LivePerson

You acknowledge that HSBC can terminate your use of Web Chat if HSBC reasonably believes that you have breached these Terms of Use.

You are not required to provide HSBC with any personal information (including sensitive information) while using this service to enquire about functionality or navigation around our website. However,

while we are responding to your enquiries or processing about your account, transaction, or application, you may be asked to provide personal and account information and location. If our system detects that you have provided a full identification number via chat services, we will perform appropriate masking to protect your personal data. Please do not disclose any of your personal or account information and location unless you have been asked by us.

For quality and verification purposes, HSBC will retain a transcript of all communications with you via Web Chat. This information will be retained by HSBC for a period of 10 years (or such other period as considered appropriate by HSBC) from the day upon which Web Chat communication took place.

Collection, use and disclosure of information

By providing us with the personal data of any third-party (including the Identifier of any intended payment recipient), you warrant and confirm you've obtained the consent of the payment recipient that their personal data can be collected, used and shared by us with any member of the HSBC Group, service providers (including third-party operators) as well as in response to any requests from any authorities.

Other important terms

You'll give us any additional information we request.

You're responsible for checking all transactions in a careful manner.

You agree that we won't be liable for any loss or damages you suffer if:

- Any event outside of our reasonable control occurs. This includes any delay or inability to act on any instructions or communications due to the breakdown or failure of the transmission or communications equipment or devices however caused or due to the interruption or delay or error in data transmission or communications.
- You've been negligent or fail to comply with these terms. For example, if you don't take precautions to ensure payments are made to the right recipients, such as checking the nickname displayed.

Your role in keeping Online and Mobile Banking safe

Your duty to take reasonable care

You must take all reasonable precautions to keep your mobile device and security information safe and prevent fraudulent use.

You'll be given a unique identifier which is your Username or Online Banking ID, Password or a Digital Secure Key. A higher level of security is required for some services. We'll let you know if this higher level applies to you. You'll need to apply for a replacement Security Key if you lose it or it breaks.

You'll follow any guidance and security measures we recommend. These include:

- Following any authentication instructions from us, including the guidance on using your Username or Online Banking ID, Password or a Security Key
- Not letting anyone else use your security details including your Username or Online Banking ID, Password or a Security Key
- Never writing down or otherwise recording your security details in a way that can be understood by someone else
- Not choosing security details that may be easy to guess
- Taking care to ensure that no one hears or sees your security details when you use them
- Not disclosing your security details to anyone
- Changing your security details immediately and telling us as soon as possible if you know, or even suspect, that someone else knows your security details, or if we ask you to
- Keeping your security details and mobile device safe
- Complying with all reasonable instructions we issue regarding keeping your security details safe
- Not leaving your mobile device unattended or letting anyone else use your mobile device
- Logging out of Online or Mobile Banking once you've finished using them
- Not leaving Online or Mobile Banking running in the background whilst logged in (for example, whilst multi-tasking, or running other apps)
- Undertaking reasonable and adequate precautions to scan for computer viruses or other destructive properties
- Checking the information you provide when you're using the Online or Mobile Banking carefully to make sure it's correct
- Only downloading our Mobile Banking app and its updates from official supplying app store and not from any unofficial sources
- Checking your records of transactions and statements and tell us straight away if there are any unauthorised transactions or discrepancies

You must not use the Online or Mobile Banking on any 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 "jailbroken" or "rooted". A jailbroken 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. Using Online or Mobile Banking on a jailbroken or rooted device may compromise security and lead to fraudulent transactions. Download and use of the Mobile Banking app on a jail broken or rooted device is entirely at your own risk and we won't be liable for any losses or any other consequences suffered or incurred by you as a result.

After initial registration we'll never contact you (or ask anyone to do so on our behalf) with a request to disclose your security details in full. If you receive a request from someone (even if they're using our name and logo and appear to be genuine) then it's likely to be fraudulent. You must not supply your security details. You should report any such requests to us immediately.

You must:

- Tell us straight away if:
 - You change your mobile number

- Your phone is lost or stolen
- Your security details become known to someone else or you suspect they are known
- Someone has unauthorised possession, control or use of your Security Key
- Tell us as soon as possible if you become aware that your services or account are being used for, or in connection, with illegal purpose or activity
- Ensure information kept on your mobile device remains secure
- Delete the Mobile Banking app from your device if you dispose of it
- Follow any other reasonable instructions we give you

You must give us information that we reasonably request so we can provide you with the services. If you don't, we may not be able to provide all the services to you. You need to ensure any information you give us is correct and up to date.

You can change your password for Online or Mobile Banking at any time using a Password Activation Request. This includes phrases, codes, numbers, or other forms of identification. When making a Password Activation Request, you'll need to give us your Username and complete your set of security questions to authenticate your request. This is part of our usual procedures.

Your new password will only be effective if it has been accepted by us.

Co-operation with investigations

You'll help us and the police in trying to recover any losses when we ask you to. This includes by:

- Facilitating our claims investigation or resolution process for any unauthorised transaction
- Making a police report
- Providing any relevant information

We may disclose information about you to the police or other relevant third parties if we think it'll help prevent or recover losses.

What happens if you don't do these things

If you don't follow our guidance above and on our website or Mobile Banking app about how to stay safe online, you may be liable for any consequences of a security breach.

We'll always verify the identity of the person giving us instructions. If you let someone use your device or your security details, we'll assume they're you and act on their instructions as if it were you. This includes allowing someone to register their biometric data on your device.

Please be aware that you may be responsible for unauthorised transactions in some circumstances. You will be responsible for any transactions on your account until you let us know that your account, security details, data or device are no longer safe.

If we reasonably believe you gave us the instruction, we will act on it. This includes if you acted fraudulently, or you were grossly negligent. If you act fraudulently or there is gross negligence on your part, you will be liable for all losses. Gross negligence can happen, for example, where you fail to keep your passwords safe or don't inform us immediately that your account is not safe. You can read more about when you're responsible for unauthorised transactions in our HSBC Account User Agreement, which you can find on our website.

Other important things

How we'll contact you

We may need to contact you from time to time. We'll contact you in any of the following ways:

SMS	We consider you've received the SMS straight after we sent it. We'll send it to the last mobile number you gave us in writing.
Email	We consider that you've received the email straight away. We'll use the last email address you gave us in writing.
Phone	We'll consider you've received our message when we tell you on a call or we leave a voicemail. We'll call you on the last mobile number you gave us in writing.
Secure message	We'll consider you have received our message straight away.
Personal delivery	We'll consider mail has been delivered at the time of personal delivery or leaving it at the address you last gave us in writing.
Prepaid post	We'll consider it received within 7 working days after sending it to the address you last gave us in writing.
Court documents	For documents relating to court proceedings (including a bankruptcy action), we'll assume you received such documents from us: <ul style="list-style-type: none">•Immediately if we leave them at your address last known to us; or•Within 7 working days if sent by prepaid registered post to your address last known to us.

We may also publish some information on our website or any digital platform. It's a good idea to check it frequently.

You'll need to give us accurate contact details otherwise we can't send you information such as transaction notification alerts.

You represent and warrant any information you give us is accurate (to the best of your knowledge).

Let us know as soon as possible if your information has changed. Going forward, you must inform us of any information changes especially relating to your change of address, signature (or your authorised signatories' signature), the authorised manner of signing or the signature requirements. We'll need a reasonable period of time (at least 7 working days) to process your change.

We can still process instructions based on your existing information or mandate.

We can use your existing contact details until we update your details in our systems. We're not responsible for any loss or damage if a third-party receives your communication.

Changes

We might change our services, how we accept instructions, operating hours or daily cut-off times without telling you first.

Sometimes we need to update our terms. We can only make changes when it's reasonable to do so.

We can't predict all of the reasons we may need to make a change, but common ones might be:

- Changes to laws or regulations
- Changes to our business, technology, services or facilities we use
- Complying with decisions or recommendations we have to follow, such as by a court, regulator or industry body or new industry guidelines or codes of practice
- To cover the increased cost of offering a product or service

You will be notified at least 60 days in advance if there any changes to our terms.

If you continue to use Online or Mobile Banking after a change to our terms, you will have accepted the change.

We send notices of change in a variety of ways, including through Online or Mobile Banking.

If you don't accept a change we've made, you can contact us and we may be able to offer you branch or phone banking as an alternative.

Our agreement

There may also be separate terms that apply to certain products or services that we supply to you. You'll need to agree to additional, separate terms for these products or services. If these terms and the separate terms say different things, then we will apply the separate terms.

We also have a privacy policy and cookie notice and you can find these on our website. These notices apply to the personal data we collect via Online and Mobile Banking. We take your privacy seriously.

Sometimes we'll offer or show third-party products or services through Online and Mobile Banking. If something goes wrong with these products or services, or you're not happy with them, we might put you directly in contact with that third-party.

You're responsible for verifying any information you use, and seeking independent professional advice on the financial, legal and tax implications of your decisions.

We'll only transfer our rights and obligations under these terms to another member of the HSBC Group or someone else we think is able to perform our obligations towards you as well as we would. We'll let you know in advance if this happens.

Sometimes one of the HSBC Group companies might need to act for us under these terms.

Joint account holders both have to comply with everything in these terms.

When we talk about 'we' 'us' or 'our' we mean HSBC Bank (Philippines) Limited.

For the Mobile Banking app, the app stores have asked us to remind you that we, not app stores, are responsible for the app. You should contact us about:

- Maintenance and support issues, or anything to do with our app's content
- Any malfunction of our app
- Any claims relating to our app

App stores are considered as third-party beneficiaries while you're using our app, and they can rely on the above terms in the same way as we can.

Intellectual property and hyperlinks

Don't alter, reverse engineer or copy all or part of our Online or Mobile Banking.

You must only use Online or Mobile Banking for making transactions, managing your account or using our services.

There might be hyperlinks to third-party websites in our Online and Mobile Banking. We're not responsible for these websites. See our hyperlink policy available on our website for more details.

"HSBC" and our hexagon logo are registered trademarks.

Apple, the Apple logo, iPhone, iPad, iPod Touch, Touch ID and Face ID are trademarks of Apple Inc. registered in the US and other countries. App Store is a Service Mark of Apple Inc.

Google Play, the Google Play logo and Android are trademarks of Google LLC.

iOS is a trademark or registered trademark of Cisco in the US and other countries and is used by Apple Inc. under license.

No links

You can't use our Online or Mobile Banking on any other website without our written consent. This includes linking another website to Online or Mobile Banking.

Suspending, restricting and ending our relationship

You can tell us at any time if you want to end this agreement and no longer use our Online and Mobile Banking services.

We can suspend, restrict or end your access to Online or Mobile Banking if:

- You:
 - Have seriously or repeatedly broken your agreement with us in these terms
 - Haven't accessed Online or Mobile Banking for a long time (for example 12 months), you can always re-register if you still need access by calling us or visiting a branch
 - No longer have a banking relationship with us
 - Use Online or Mobile Banking for business purposes

- Use Online or Mobile Banking for any illegal purposes or otherwise in an abusive, libellous, obscene or threatening way
- We:
 - Have evidence of a breach of security or misuse of your account or security details
 - Reasonably believe it's necessary to keep your account safe, this includes if you've downloaded or installed any malware or other software that could compromise the security of your device or account
 - Otherwise reasonably believe such action is required

Sometimes we might need to suspend, restrict or end your access to Online or Mobile Banking immediately without telling you first. Also, we may not be able to tell you the reason why.

We won't be responsible for any losses caused by us suspending, restricting or ending your access to Online or Mobile Banking.

You can use phone banking or visit one of our branches if you no longer have access to, or are having difficulty with, Online or Mobile Banking.

If your access to Online or Mobile Banking is suspended, restricted or ends:

- We may have to also close any accounts, products or services that are only available via Online or Mobile Banking
- You'll no longer receive statements digitally and you'll need to make sure we have your up to date details so that we can start sending statements to you by post

You should delete the Mobile Banking app from your device if our relationship ends.

Our liability

We won't be responsible for any issues caused by third-party services or software, for example instant messaging or video chat apps, etc. used with our accounts or services whether because of a delay in processing information or other issues unless:

- We provided you with such third-party services or software
- Such issues are caused by our mistake

We won't be responsible for any issues caused by:

- Acting on, or failing to act on, instructions which are incomplete, inaccurate or that we do not understand
- Any delay in acting on instructions, information or communication via Online or Mobile Banking where this is caused by events outside of our reasonable control
- Recovery or attempts to recover any amounts you owe us
- Enforcement of these terms
- You installing any malware on your device
- Your reliance on any third-party information feeds (this includes stock quotes and foreign exchange rates) materials, products or services

- Any breach or failure to-observe any of these terms by you or any other unauthorised person using your security details including your Username, Online Banking ID, Password, Password Reset Questions and Security Key.

We'll only be responsible for direct loss in connection with Online or Mobile Banking if it was caused:

- Because we, or someone acting for us, acted negligently (this basically means where we didn't take proper care where we should have done) or fraudulently (this basically means being deceitful). This includes our employees, agents, information providers or the HSBC Group involved in the provision of Online or Mobile Banking;
- By faults in our systems unless they are obvious or we've given notice about them. This includes systems we use to provide Online and Mobile Banking.
- By unauthorised transactions occurring before you've established a Username, Online Banking ID and Password
- By unauthorised transactions conducted via Online or Mobile Banking as a result of a computer crime which should have been prevented by our risk control and management measures
- Because we failed to do something we agreed to do in these terms and the resulting loss you suffered was of a type and amount we could have expected as a result of those actions or failures

You won't be responsible if it's reasonably clear that you couldn't have contributed to the loss.

There are other places in these terms where we say we're not responsible for any losses – this is always subject to the above unless we say otherwise.

Confidential information

Information we provide via Online and Mobile Banking is confidential to us, the HSBC Group and any of our relevant third-party information providers. You don't own or have rights over this confidential information or Online and Mobile Banking which means you must not:

- Share it with others unless you legally must
- Download, copy or sell it
- Remove or change our branding such as our trademark or copyright notice
- Combine or include it with other content;
- Represent or infer you own it in any way

You don't own and have no right, title or interest to our confidential information, or any related copyright, patent, trademark, service mark, proprietary property, trade secret or exclusive work.

All ownership of Online and Mobile Banking remains with us.

Records

Our internal records will take priority over any other records or information about your account.

We can rectify any error which occurs in our systems or information or take any action as appropriate on a case-by-case basis.

Severability

If part of our terms or all of it becomes invalid, illegal or unenforceable under the law of any jurisdiction, that won't affect or impair the validity, legality and enforceability of such provision in any other jurisdiction or the remaining provisions of this agreement or any part it.

Survival on termination

To the extent permissible by applicable law, the content of these terms will continue to apply after it has been terminated or your deposit account has been closed.

No waiver

If you breach these terms, we may not take steps to enforce our rights straight away. We can decide when to take these steps. Any delay is not a waiver of our rights.

We'll only waive our rights in writing.

All rights cumulative

The rights and remedies in these terms are cumulative and not exclusive of any other rights or remedies (whether provided by law or otherwise). This means we can choose more than one right or remedy to enforce. We can also choose a number of rights or remedies over time.

Governing law and jurisdiction

We hope that we're always able to resolve issues between us. If we can't and we end up going to court, the services and these terms and conditions shall be governed by and construed in accordance with the laws of the Philippines. Each of the Bank and the customer submits to the non-exclusive jurisdiction of the Courts of the Philippines but these terms and conditions may be enforced in the courts of any competent jurisdiction.

Glossary

In these terms, references to:

Account

Means the bank accounts with us that are associated with the username / online banking ID, password and Security Key issued to you for the services.

Authorities

Means any judicial, administrative or regulatory body, any government, or public or government agency, instrumentality or authority, or any domestic or foreign tax, revenue, fiscal or monetary authority or agency, securities or futures exchange, self-regulatory organisation, trade repositories, court, central bank or law enforcement body, or any agents thereof, having jurisdiction over any part of HSBC Group.

Contract

Means the contract entered into between us and you when you accept these terms.

HSBC Group

Means HSBC Holdings plc, and/or any of, its affiliates, subsidiaries, associated entities and any of their branches and offices, and "any member of the HSBC Group" has the same meaning.

Including

Means including, without limitation to the generality of the surrounding words.

Information provider

Means a third-party from whom we source information that we may provide to you as part of the services.

Instructions

Is any request or instruction to us, which is issued through the use of one or more of the Username, Online Banking ID, Password, Password Reset Questions, Security Code and any other identifiers prescribed by us from time to time.

Mobile Banking

Means the mobile banking service and all content, services and/or functions made available therein provided by us to you through the application branded as HSBC Mobile Banking or such other applications as may be designated by us from time to time for use on mobile devices, through which you can access some of our Online Banking services. The Mobile Banking app can only be downloaded to a mobile device which runs on operating systems as may be prescribed by us from time to time.

Mobile Banking app

Means the HSBC Mobile Banking application (as updated from time to time) which can be downloaded to any mobile device which runs an operating system supported by us, through which you can access some of our Online Banking services.

OFR

Also known as "Password Activation Request" is a process whereby you reset your Password offline. In this process, you are required to write in to us for approval to reset your Password.

OLR

Also known as "Online Password Reset" is a process whereby you reset your Password online.

Online Banking

Means the online banking service and all content, services and/or functions made available therein provided by us to you through <https://www.hsbc.com.ph/> or such website, channel or other electronic means as we may prescribe from time to time, which may allow you to electronically access your accounts and any information related thereto and give instructions in respect of certain products or services provided by us to you.

Password

Includes all confidential passwords, phrases, codes, numbers, or other forms of identification issued to you or designated by you and, which may be used by you to access Online Banking and Mobile Banking.

Password reset questions

Refers to a set of security questions you have selected and the corresponding security answers you have provided to us during your Online Password Reset.

Personal data

Means any data relating to an individual, whether true or not, from which the individual can be identified, whether with other data or other information the Bank is likely to have access to or otherwise, including, without limitation, sensitive personal data.

Services

Refers to the services provided by us to you through any one or more of the following:

- Online Banking
- Mobile Banking

From time to time and by which you may access information and give us Instructions in respect of certain of your accounts with us, as well as the applications, content, services and/or functions made available thereunder by or on behalf of us from time to time.

Security code

Means a one-time password generated by the Security Key.

Security Key

Means the physical electronic device or digital security key designated by us for use by you to generate Security Codes (one-time passwords) to access and transact Online Banking and Mobile Banking services.

Terms

Means these terms and conditions and any supplementary terms and conditions which we notify you of under clause "Changes", as may be amended from time to time.

Username/Internet Banking ID

Is the unique identifier, by whatever name called, which is selected by you in connection with the services.

"you", "your" and "yours"

Means you, our customer or the person who has downloaded or used the Mobile Banking app. Where more than one person is authorised to operate an account, every reference in these terms to "you" is deemed to include each and all of the account holders and each and all of the persons authorised to operate the account, and all of you are jointly and severally liable under these terms.

"we", "us", "our" and "the Bank"

Means HSBC Bank (Philippines) Limited and its successors and assigns.