HSBC Online Banking

Combined Product Disclosure Statement
and Supplementary Product
Disclosure Statement

HSBC

IMPORTANT NOTICE:

Notice of Change to the HSBC Online Banking Combined Product Disclosure Statement and Supplementary Product Disclosure Statement.

The following changes are made to the "HSBC Online Banking Combined Product Disclosure Statement and Supplementary Product Disclosure Statement" and is effective on 21 January 2018.

- Removal of "Touch ID" in Part A - 1.1 Defined terms.
- Removal of "Touch ID" reference in Part A - 2.6 Online Banking Service security, bullet point (d).
- The addition of section 8 "HSBC Mobile Banking App", which contains new clauses 8.1 to 8.7.13 in Part A below.
- All page numbers in the HSBC Online Banking Combined Product Disclosure Statement and Supplementary Product Disclosure Statement are re-ordered accordingly.

PART A

HSBC Online Banking Product Disclosure Statement

The Date of this PDS is 21 January 2018.

This Product Disclosure Statement contained in Part A applies to and must be read by all customers who use the Online Banking Service.

PART B

Supplementary Product Disclosure Statement

The Date of this SPDS is 1 August 2017.

The Supplementary Product Disclosure Statement contained in Part B only applies to HSBC Premier Customers. Part B does not apply to, and need not be read by, a customer who is not an HSBC Premier Customer.

PART C

Supplementary Product Disclosure Statement

The date of this SPDS is 1 August 2017.

The Supplementary Product Disclosure Statement contained in Part C only applies to HSBC Entity Customers. Part C does not apply to, and need not be read by, a customer who is not a HSBC Entity Customer.

CONTENTS

PART A: ONLINE BANKING PRODUCT DISCLOSURE STATEMENT

PART C: SUPPLEMENTARY PRODUCT DISCLOSURE STATEMENT FOR HSBC ONLINE BANKING

PART A

HSBC Online Banking Product Disclosure Statement

KEY FEATURES

The Online Banking Service is a service that HSBC makes available through the internet network to enable the electronic receipt and transmission of information and instructions (including in relation to a linked account held with HSBC).

It is an alternative way to do your banking, 24 hours a day, 7 days a week. When Users log-in to the Online Banking Service, depending on the Electronic Equipment they use and the way in which they elect to access the Online Banking Service, they can perform the following:

- Check the balance of linked accounts held with HSBC
- Check Credit cards and loan accounts balance
- Check currency rates
- Transfer funds to any accounts within HSBC
- Transfer funds to other accounts in Australia and overseas
- Set up and manage recurring payments
- Manage your secure key
- Pay bills displaying the Bpay® symbol
- Download or a copy of a previous transaction history. Stop or cancel a cheque
- Change your Password
- Place an order for the purchase or sale of foreign currency which is to be transferred between linked accounts held with HSBC
- Request a document, staff contact or interview with an HSBC representative
- Send secure messages to HSBC via the Online Banking secured site
- Update Personal Information.
- View E-Statement for all products in one place: Supports both Banking & Credit Card/ Personal Loan

(Note: Depending on the account you hold you may not be able to access all the above features. Service features may be amended and may change from time to time.

Also, depending on the type of Electronic Equipment that you elect to use to access the Online Banking Service, you may not be able to access all of the above features. For example, if you elect to access the Online Banking Service via a smart phone or other similar mobile device, then depending on your smart phone or mobile device, its compatibility with our Online Banking Service and the way in which you elect to access the Online Banking Service, some of the above features may not be available.)

SIGNIFICANT RISKS, COSTS, COOLING-OFF AND TAXATION

Significant risks

It is important to keep safe any secret codes such as the PIN, and Password and, if you have been issued a Secure Key for use with the Online Banking Service, the Secure Key and the Security Code.

You should consider the inherent risks in sending instructions, passwords and updating your details by email. You need to consider the security of the email and ensure you are only connecting to http://www.hsbc.com.au

You should also be aware of internet and email scams which may mislead you into providing your financial details to an unknown party.

You are responsible for acquiring and maintaining any equipment required for continued access to and use of the Online Banking Service. All reasonable steps must be taken to protect the Electronic Equipment hardware and software including ensuring that the Electronic Equipment is free of viruses.

In accessing the Online Banking Service via telecommunication equipment, you should be aware that a communications line failure will impact your ability to access the system. This could result in delays in receiving account information and delivering transactions to HSBC.

HSBC will not be responsible for any losses suffered by you as a result of line failure.

Costs

HSBC regularly reviews the fees and charges that apply to its financial services to ensure that its products and services remain competitive. For that reason, the specific fees applicable to the Online Banking Service are set out in the relevant fees and charges guide. This document forms part of this Product Disclosure Statement and therefore should be read in full before you make a decision to use the Online Banking Service.

If you need another copy of the fees and charges guide, please ask a staff member of any HSBC branch, for a copy or call our Direct Service Centre on 1300 308 008. If you have a relationship manager, please ask your relationship manager for a copy of the fees and charges guide.

Cooling off

There is no cooling-off regime that applies to the Online Banking Service.

ACCESS TO THE ONLINE BANKING SERVICE

Access to the Online Banking Service is only available if you have, or a User has on your behalf:

- **agreed** to receiving notices regarding the Online Banking

Service by Electronic Communication.

A User's election to receive notices regarding the Online Banking Service by electronic communication will constitute your agreement to receive notices regarding the Online Banking Service by Electronic Communication to the email address nominated by the User.

In order for you to receive electronic notices, a User will need to provide HSBC with a nominated email address. The nominated email address may be changed at any time by a User.

If HSBC has already received an email address from a User, HSBC will consider that email address to be the nominated email address for the purposes of you receiving electronic notices. If HSBC has not already received a nominated email address, a User can provide us with an email address by calling HSBC or by completing and sending us a form available on www.hsbc.com.au.

After HSBC is provided with a nominated email address, HSBC can notify you of ongoing changes to the Online Banking Service by sending an email that contains the communication to the nominated email address, or by sending an email to the nominated email address alerting the User to retrieve the communication on www.hsbc.com.au and/or by accessing the Online Banking Service, as advised. You must ensure that the nominated email address remains valid at all times.

When you opt-in to receive notices regarding the Online Banking Service by Electronic Communication and HSBC is provided with a nominated email address, you will not receive paper notices. If a User does not provide HSBC with a nominated email address, the User will receive notices by non-electronic means. If you terminate your agreement to receive notices by Electronic Communication, HSBC reserves its right not to provide access to the Online Banking Service.

AND

- **accepted** the terms and conditions applying to the Online Banking Service as contained in this Online Banking Product Disclosure Statement (the "Terms") by clicking on the "Accept" button presented to a User when a User first logs-in to the Online Banking Service and/or when these Terms are amended. If the Terms are accepted by a User, you warrant that the User is authorised to accept the Terms on your behalf.

OTHER PRODUCT DISCLOSURE STATEMENTS

You should read these terms in conjunction with the Product Disclosure Statements applying to your EFT Accounts accessed via the Online Banking Service.

ABOUT THESE TERMS

These Terms apply to the Online Banking Service (including use of the Online Banking Service to make a BPAY® Payment).

The Online Banking Service provides you with access to your EFT Accounts.

These Terms operate in conjunction with the terms and conditions applicable to EFT Accounts you access using the Online Banking Service. If there is an inconsistency, these Terms prevail in respect of EFT Transactions (as defined).

Other terms and conditions may apply by operation of a relevant statute or the Code of Banking Practice.

Please read these Terms before using the Online Banking Service.

If you do not understand any part of them, or if you have any questions, please speak with a staff member at any HSBC branch or call our Direct Service Centre on 1300 306 543.

Customer Service and Enquiries
1300 306 543 Monday to Friday from 8am to 8pm or +61 29005 8421 if calling from overseas.

Lost or Stolen PINs or Secure Keys or Suspected Unauthorised Transactions Online Banking only or Mistaken Internet Payments 1300 306 543

1. GENERAL TERMS AND CONDITIONS

1.1 Defined terms

The following terms have the following meaning where used anywhere in these terms and conditions.

"Access Method" means a method that we make available to Users of the Online Banking Service and accept as authority to act on an instruction given through Electronic Equipment. A reference to an Access Method includes a reference to each of its individual components and includes, but is not limited to an Identifier (including a Username), a PIN, PBN, a Security Code, a Username, a Password or any combination of these.

"ADI" means an authorised deposit-taking institution as defined in the *Banking Act 1959* (Cth).

"Bank@Post™" means Australia Post's banking service.

"Banking Day" means, for any purpose, any day other than a Saturday or Sunday on which one or more branches of HSBC are open in Australia and, if the EFT Account is in a currency other than Australian

Dollars, which is also a day other than a Saturday or Sunday on which banks are open for business in any place with which HSBC needs to communicate or effect or arrange any payment, currency conversion or other transaction for that purpose.

"Biller" means an organisation which tells you that you can make payments to it through the BPAY® Scheme.

"BPAY® Payment" means a payment you instruct HSBC to make on your behalf to a Biller through the BPAY® Scheme.

"BPAY® Scheme" means an electronic payments scheme through which you can ask HSBC, while HSBC remains a member of the scheme, to make payments on your behalf to Billers. HSBC will tell you if it ceases to be a member of the scheme.

"Credit Card Account" means an account established in your name for recording all transactions in connection with the HSBC Credit Card Contract.

"Credit Card Contract" means the credit card opening document you signed and the Conditions of Use as varied from time to time.

"Digital Secure Key" is a feature within the HSBC Mobile Banking app. It fulfils the same function as the physical Secure Key allowing the customer to log on to their mobile banking app with full security.

"EFT Account" means an account you have with HSBC which you nominate and which HSBC authorises you to access via the Online Banking Service and/or to conduct EFT Transactions. For the avoidance of any doubt, EFT Accounts also include Loan Accounts created pursuant to the HSBC Personal Loan Contract and Credit Card Accounts. If there is more than one EFT Account holder and/or more than one authorised signatory to the EFT Account, each EFT Account holder and each signatory must be authorised to operate the EFT Account alone. For the avoidance of doubt, EFT Accounts also include Loan Accounts and Credit Card Accounts.

"EFT System" means the shared system under which EFT Transactions are processed.

"EFT Transaction" means an electronic funds transfer from or to an EFT Account initiated by a User through Electronic Equipment using an Access Method.

"Electronic Communication" means a message HSBC transmits to a User and the User receives from HSBC electronically, in a form that the User can retain for later reference such as by printing or by storing for later display or listening.

"Electronic Equipment" includes, but is not limited to, a computer and telephone used for Online Banking.

"Group" means, in relation to HSBC, all of its offices, branches, holding companies, subsidiaries, affiliates and any other entity of which HSBC Holdings plc owns (directly or indirectly) 50 per cent or more of the issued voting share capital or stock.

"**HSBC Personal Loan Contract"** means the letter you signed and the HSBC Personal Loan Contract Standard Terms and Conditions as varied from time to time.

"HSBC, we, our or us" means HSBC Bank Australia Limited.
ABN 48 006 434 162 AFSL 232595.

"Identifier" means information which must be provided to access your EFT Accounts using Electronic Equipment. An Identifier includes, but is not limited to, the PBN and Username.

"Instruction" means any request or instruction to HSBC which is effected through the Online Banking Service by use of an Access Method.

"Online Banking Service" means the service that HSBC makes available through the Internet network to enable the electronic receipt and transmission of information and instructions (including in relation to an EFT Account).

"Loan Account"means an account HSBC establish in your name for recording all transactions in connection with the HSBC Personal Loan Contract.

"Mistaken Internet Payment" means a payment made by a User through 'Pay Anyone' where funds are paid into the account of an Unintended Recipient because the User enters or selects a bank/state/branch (BSB) number and/or account number that does not belong to the named and/or intended recipient as a result of:

(a) the User's error; or

(b) the User being advised of the wrong BSB number and/or account number.

This does not include BPAY® Payments.

"Password" means the code comprising alpha-numeric characters chosen by a User to be used with the Username to access the Online Banking Service.

"Pay Anyone" means a facility within the Online Banking Service which allows a User to make payments to other HSBC accounts or accounts held at other Australian financial institutions.

"Payment Cut-off Time" means the time in Sydney at which HSBC will not process or make any further payments in that currency on that day. The cut off time varies between currencies. The list of specific cut off times for specific currencies is available at www.hsbc.com.au.

"PBN" means the ten digit Personal Banking Number supplied to a User

and by which HSBC identifies a User for Online Banking.

"PIN" means the personal identification number provided by HSBC to you for use as an access code when registering for the Online Banking Service.

"Receiving ADI" means an ADI which has subscribed to the ePayments Code and whose customer has received an internet payment.

"Security Code" means an unpredictable code generated by a Secure Key at predetermined intervals, to be used, in conjunction with a Username and Password, to access the Online Banking Service. Once a User has accessed the Online Banking Service, HSBC may ask the User to enter the Security Code a further time to confirm some transactions. If the Secure Key is misused, lost, stolen or the Security Code is allowed to be seen by a person other than the relevant User, the protection provided by the Security Code will be diminished or the protection will no longer be effective.

"Secure Key" means the physical device which HSBC may provide to each User or the HSBC mobile app (Digital Secure Key), which generates a new Security Code at predetermined intervals. The Secure Key remains HSBC's property at all times.

"Sending ADI" means an ADI which has subscribed to the ePayments Code and whose customer has made an internet payment.

"Service" means the Online Banking Service.

"Terms" means these terms and conditions, as amended from time to time.

"Unauthorised" means without the knowledge or consent of a User.

"Unauthorised EFT transaction" means an electronic funds transfer from an EFT Account initiated through Electronic Equipment using an Access Method without your knowledge or consent.

"Unintended Recipient" means the recipient of funds as a result of a Mistaken Internet Payment.

"User" means you and any other person authorised by you and HSBC to use the service to access and operate an account alone.

"Username" means the code comprising alpha-numeric characters set up by a User to be used with the Password and Security Code to access the Online Banking Service.

"you" or **"your"** means the person(s) named as customer in the relevant EFT Account opening document and where the context permits if there is more than one person named as customer or EFT Account holder, references to you mean each person separately and

every two or more persons jointly. Any other grammatical forms of the word "you" have corresponding meaning.

1.2 ePayments Code

HSBC warrants that it will comply with the requirements of the ePayments Code, where those requirements apply to your dealings with it.

1.3 Code of Banking Practice

HSBC warrants that it will comply with the requirements of the Code of Banking Practice where those requirements apply to your dealings with it.

1.4 Acceptance

You agree to these Terms when, having been presented with these Terms on our website (www.hsbc.com.au), a User clicks the "Accept" button indicating acceptance of the Terms.

1.5 Records and statements

HSBC will provide a statement of account for your EFT Accounts at least every 6 months. You may request more frequent EFT Account statements and you may also request an EFT Account statement at any time. HSBC may charge a fee for issuing a replacement or duplicate statement of account, as advised in its booklet ***"Personal financial services charges – your guide."***

You should carefully check EFT Account records and statements when you receive them. If you believe that there has been a mistake in any transaction using the Online Banking Service or an Unauthorised EFT Transaction, you must notify HSBC immediately by calling 1300 306 543. HSBC's records, unless proven to be wrong, will be evidence of your dealings with HSBC in connection with the Online Banking Service.

1.6 Fees and Charges

If the Online Banking Service is used to effect a transaction you may incur a fee and/or government charge, tax or duty on the EFT Account you access. HSBC may also charge you a fee for the issue, use, renewal and replacement of an Access Method. The fees and charges payable in respect of the Online Banking Service are detailed in HSBC's ***"Personal financial services charges – your guide."*** (at the time the relevant transaction is undertaken), available from any HSBC branch or at www.hsbc.com.au

1.7 Changes to Terms

HSBC reserves the right to change these Terms and any other information it has issued about the Online Banking Service at any time.

Where a change imposes or increases a fee or charge, we will give you notice in writing at least 30 days before the change comes into effect.

We will give you notice in writing at least 20 days before the change

comes into effect (or such longer period required by law or, if applicable, the Code of Banking Practice) if we:

- impose, remove or adjust a daily or other periodic transaction limit applying to the use of an Access Method, an EFT Account or Electronic Equipment; or
- increase your liability for losses relating to EFT Transactions.

Subject to any applicable legislation or Code, we will give you notice of other changes no later than the date on which the change takes place in writing or by publishing an advertisement, except where an immediate change is necessary to restore or maintain the security of the EFT system or individual EFT Accounts.

Written notice under this clause 1.7 may be given electronically in accordance with clause 1.11.

1.8 Additional Users

If HSBC agrees, you may authorise another person to access and operate your EFT Accounts using the Online Banking Service.

If requested by you, HSBC will provide Users with an Access Method to access your EFT Accounts. A User's access to your EFT Accounts using the Online Banking Service is governed by the relevant provisions of these Terms. HSBC suggests you provide all Users with a copy of these Terms. You must ensure that each User protects their Access Method in the same way these Terms require you to protect your Access Method.

You will be liable for all transactions carried out on your EFT Accounts by any person authorised by you.

Your cancellation of a User's authority will not be effective until your notification of the cancellation is received by HSBC.

1.9 Agreed limits

Users must not use an Access Method to withdraw funds in excess of any limit agreed with HSBC. If an EFT Account goes over the agreed limit, HSBC may permit a User to use the Access Method, but you must deposit funds to bring the EFT Account within its agreed limit without unreasonable delay. There are 4 types of daily transaction limits applicable to each User.

The maximum daily transaction limits are:

	Maximum daily limits*
Transfers between EFT Accounts ^ (including foreign currency transfers**)	$500,000
Transfers between EFT Accounts and: • third party accounts (including third party HSBC accounts) and • accounts you may have with another HSBC entity or other financial institutions [these transfers include foreign currency transfers but exclude transfers to pre-designated accounts]	Default limit is $50,000
Transfers between EFT Accounts and pre-designated third party accounts including a pre-designated HSBC EFT Account in Australia** (including foreign currency transfers)	This facility is only available on request. Should we make this facility available to you, the default limit is $100,000. The maximum limit you may request is $250,000.
BPAY®	$25,000

* The maximum daily limit figures in this table refer to the daily limits that apply to each User. For example, if you have two Users, each User may each effect daily transfers "between EFT Accounts" of up to $500,000.

** The maximum foreign currency transfer Instruction limit is $50,000 per Instruction where instantaneous real-time pricing is not available. Where a foreign currency transfer Instruction is provided after the relevant Payment Cut-off Time, HSBC will apply the currency exchange rate that applies at the time of the Instruction in order to calculate the Australian dollar value for the purposes of daily transaction limits. However, when HSBC processes the Instruction HSBC will apply the currency exchange rate that applies at the time of the processing and that exchange rate may be different from the exchange rate that applied at the time the Instruction was provided.

^ This includes transfers between your Serious Saver Account and your Nominated Account.

N.B. Daily transactional limits apply to all fund transfers, including 'Pay Later' and recurring transfers. For example if today you initiate a 'Pay Later' transfer of $20,000 or a recurring transaction of $5,000 over the next 4 weeks, then in both these instances the total funds transfer amount of $20,000 will apply to your transaction limit today. Contact us if you'd like to request an increase to your daily limit.

All amounts are in Australian Dollars and may change from time to time.

Merchants, our agents and other financial institutions may impose their own restrictions on the amount of funds that may be withdrawn, paid or transferred.

1.10 Termination

You may stop your use of the Online Banking Service at any time by giving written notice to HSBC.

HSBC may terminate the Online Banking Service at any time by giving you a written notice. HSBC may suspend or cancel an Access Method at any time without notice if it believes the Access Method or Secure Key is being misused, there is a concern as to the security of the

Access Method or Secure Key or there is noncompliance with these Terms.

When an Access Method has been cancelled by you or HSBC, Users must not attempt to use the cancelled Access Method again. If de-activated, the Secure Key must be returned by you and/or your additional User(s) upon HSBC's request.

Bill payments or funds transfers for which Instructions have been given and which are scheduled to be made after your use of the Online Banking Service is terminated may not be effected by HSBC.

1.11 Electronic communications

The Online Banking Service is only available where you agree that HSBC may satisfy any requirements under these Terms and ePayments Code to provide Users with information by:

(a) sending an email to an email address nominated by the User; or

(b) making the information available at our website www.hsbc.com.au, or through the Online Banking Service, for retrieval by a User (after notifying the User by email to the User's nominated email address that the information is available for retrieval and the nature of the information and providing the User with the ability to retrieve the information through our website or through the Online Banking Service).

If you agree to the above, then:

a) if a User has provided a nominated email address, the User will not receive paper copies of the relevant information;

b) the User will need to regularly check to see if he or she has received any emails from us;

c) the User will need to maintain and check his or her Electronic Equipment and his or her electronic address regularly to ensure it is always capable of receiving an Electronic Communication; and

d) the User will be responsible for printing or saving important information – and we strongly recommend that Users do so.

You may at any time by notice to HSBC terminate your agreement to receive information by Electronic Equipment or Electronic address. If a User does not provide HSBC with a nominated email address, the User will receive notices by non-electronic means. If you terminate your agreement to receive notices by Electronic Communication HSBC reserves its right not to provide you with access the Online Banking Service. If this occurs HSBC will advise you that the Service has been terminated.

1.12 Telegraphic Transfers

Where you request an outward Telegraphic Transfer (TT) to be effected from an account you acknowledge and agree that the following applies:

a) In the absence of any specified instructions to the contrary, HSBC may either effect a TT in the currency of the country in which payment is to be made or at HSBC's sole discretion, choose not to effect the TT until further instructions are obtained from the User in which case, HSBC will not be responsible for any loss or delays which you may suffer.

b) Unless you provide instructions to the contrary, all charges incurred outside Australia are for the account of the beneficiary.

c) HSBC reserves the right to draw any TT on a different place from that specified by you if operational circumstances so require.

d) Payment requests delivered to HSBC (in any form including electronically or otherwise), are subject to cut off times. These cut off times vary depending on the geographical location of the destination and are subject to change from time to time. A list of cut off times is available from HSBC on request.

e) Any requests received by HSBC within the cut off time for the relevant currency, will be processed on the requested value date. However, while HSBC will remit your funds on the value date, HSBC cannot confirm the actions of the receiving bank nor guarantee that the funds will be received by the beneficiary on the same day. Funds sent by TT will usually be received by the beneficiary bank within 48 hours from the time the TT is processed. HSBC will not be liable for any delays in processing by the beneficiary bank.

f) Any requests received by HSBC after the cut off times for the relevant currency, will not be processed on the same day.

g) Where HSBC are unable to provide a firm exchange rate quotation at the time of the User's request for a TT, HSBC will provide you with a provisional exchange rate. However, HSBC will effect a TT on the basis of our actual selling rate for the relevant currency against the AUD (or another currency in which your EFT Account is denominated where applicable) at the time of processing the TT. The applicable amount will be debited from your account at the time the TT is processed.

h) TTs are dispatched entirely at your own risk.

i) HSBC is at liberty to send any TT either literally or in cipher and we accept no responsibility for any loss, delay, error, omission or mutilation, which may occur in the transmission of any message or for its misinterpretation when received.

j) You may only cancel or amend a TT if HSBC agrees in our absolute discretion.

k) In effecting a TT from an EFT Account, HSBC may be required by law or other rules, policies or guidelines by which HSBC is bound, to disclose certain information which HSBC holds about the User to the beneficiary and/or the beneficiary's bank or intermediary service providers in the course of effecting the payment, and by requesting us to perform the TT, you consent to HSBC's disclosure of your information.

l) Where you receive an inward payment into your account by way of TT and that payment is made in a foreign currency, HSBC will convert that payment into AUD unless your account is denominated in that currency.

m) Fees and charges are payable in respect to your receipt of an inward or request for payment of an outward TT. These are set out in HSBC's separate document ***"Personal financial services charges - your guide".***

1.13 Contact

You can contact HSBC by:

(a) telephoning us on 1300 306 543; or

(b) writing to us at GPO Box 5302, Sydney NSW 2001.

HSBC may write to you at the address currently recorded on its system, or in accordance with the section of these Terms headed "Electronic communications".

1.14 Governing Law

HSBC's agreement with you on these Terms and the transactions carried out under it are governed by the law in force in the State of New South Wales, Australia. Both you and HSBC submit to the non exclusive jurisdiction of the courts of that State in respect of any dispute.

2. ONLINE BANKING SERVICE

2.1 About these Terms

These Terms apply to all transactions involving the use of the Online Banking Service to access your EFT Accounts.

2.2 Use of the Online Banking Service

2.2A Use of the Online Banking Service in relation to Credit Card Accounts and Loan Accounts

Without limiting sub-clause 2.2 "Use of the Online Banking Service", your use of the Online Banking Service for the Credit Card Account and/or Loan Account is limited to:

(a) viewing and obtaining the balance of your EFT Account;

(b) View transactions

(c) View account details

(d) Download statements

(e) Opt-in or opt-out of e-statement

(f) Download transactions

(g) opening new HSBC Personal Deposit Accounts with HSBC, send Electronic Communications to HSBC, receive Electronic Communications from HSBC and change Passwords.

Depending on the type of Account and the Electronic Equipment that is used to access the Online Banking Service, the Online Banking Service can be used to:

(a) obtain the balance of any EFT Account,

(b) transfer funds to any EFT Account or other account,

(c) transfer funds from any EFT Account,

(d) request copies of previous statements in relation to any EFT Account,

(e) stop cheques drawn on any EFT Account,

(f) to make, view, amend and delete electronic standing order payment instructions in relation to any EFT Account,

(g) make BPAY® payments from any EFT Account,

(h) change the personal details (including email address, telephone and fax numbers, mailing address, date of birth, annual personal income, number of dependents, occupation and name of employer) held by HSBC for any EFT Account;

(i) make a request for a brochure, staff contact or interview with an HSBC representative,

(j) subject to future payment instructions not applying to a specific EFT Account – select or de-select specific EFT Accounts to be linked to the Online Banking Service; and

(k) place orders for the purchase or sale of foreign currency provided that the currency purchased is to be transferred between EFT Accounts. If placing orders for the purchase or sale of a foreign currency in excess of any limit advised by HSBC from time to

time, any rates disclosed will be indicative only.

2.3 Access to Online Banking Service

You agree that any person who supplies HSBC with:

(a) if HSBC has issued a User with a Secure Key, the User's PBN, PIN and Security Code; or,

(b) if HSBC has never issued a Secure Key to a User, the User's PBN and PIN, will be asked to set up a Username and Password.

Once a Username and Password has been chosen by a person, you agree that when that person supplies HSBC with:

(i) if HSBC has issued a User with a Secure Key, the User's Security Code and the Username and Password; or

(ii) if HSBC has never issued a Secure Key to a User, the User's Username and Password, that person may be allowed access to the Online Banking Service and to any EFT Account.

Once a User has accessed the Online Banking Service, HSBC may ask the User to enter the Security Code (if the User has been issued with a Secure Key) a further time to confirm some transactions. If HSBC does so, you acknowledge that HSBC will not carry out the transaction unless the correct Security Code is supplied to it a further time.

You agree that HSBC may delay acting upon an Instruction or ask for more information before acting on an Instruction.

Whilst HSBC may specify limits on transaction types and values in respect of certain EFT Accounts or the use of the Online Banking Service, you may use the Online Banking Service to decrease the transaction limit otherwise applicable to any EFT Account. Please note that HSBC may refuse to act on an instruction if a transaction exceeds a particular limit - whether that limit is set by HSBC or you. Please refer to HSBC's Online Banking Limits for details of limits imposed upon the Online Banking Service. When BPAY® payments are made, other participants in the BPAY® scheme may impose additional restrictions.

Where HSBC has Instructions for more than one payment from an EFT Account, it will determine the order or priority in which the payments are made.

HSBC may change a User's PBN or PIN at any time, by notifying the User in writing. Users may change their PIN for use with Phone Banking, or Password at any time.

2.4 Processing Instructions

If a User gives an Instruction to make an Australian Dollar transfer between any EFT Accounts with HSBC on

a day when any branch of HSBC is open for business it will be made on that day. If no branch of HSBC is open for business the transfer will be made on the next day upon which such a branch is open for business.

If a User gives an Instruction to make an Australian Dollar transfer from an EFT Account to an account not held with HSBC on any day which is not a Banking Day it will not be made until the next Banking Day.

If a User gives an Instruction on a Banking Day to make an Australian Dollar transfer from an EFT Account after the Payment Cut-off Time it may be processed on the next Banking Day.

If a User gives an Instruction to transfer a currency (other than Australian Dollars) after the Payment Cut-off Time, it will be made on the next day which is both a Banking Day and a day upon which banks in the country of the relevant business are open for business other than a day which is Saturday or Sunday in Australia.

A BPAY® Payment may take longer to be credited to a Biller if a User gives an Instruction to make the payment on a day which is not a Banking Day or if another participant in the BPAY® Scheme does not process the request as soon as they receive its details.

2.5 Electronic advertising

From time to time HSBC may advertise its own products or services and those of other companies in the Group on the website through which the Online Banking Service is accessed. If, in relation to other agreements between you and HSBC, you have asked HSBC not to send you any marketing material (or if you do so in the future), you agree that this restriction will not apply to these electronic advertisements and you consent to receiving them when accessing HSBC's Internet website and/or Online Banking Service.

2.6 Online Banking Service security

HSBC uses a very high level of encryption to protect transactions and your EFT Accounts from Unauthorised access. The use of such levels of encryption may be illegal in certain jurisdictions. It is the responsibility of the User to ensure that the User's ability to use the Online Banking Service is permitted by local law and HSBC shall not be liable for any loss or damage suffered by a User as a result of not being able to use the Online Banking Service in these jurisdictions.
Users are responsible for acquiring and maintaining any Electronic Equipment required for continued access to and use of the Online Banking Service, and for the User's own Electronic Equipment anti-virus and security measures. Users must take all reasonable steps to protect the security of their Electronic Equipment hardware and software and their Access Method, including by ensuring:

(a) their Electronic Equipment is free of viruses;

(b) their Electronic Equipment is not left unattended while they are logged on to the Online Banking Service;

(c) their Electronic Equipment is free of any form of program or mechanism capable of recording the PIN, Username and/or Password; and

(d) they shut down all windows of the browser used to access the Online Banking Service and that the "back" function or similar function cannot be used to trace their activities.

(e) If we identify or detect that your device has been modified from the original (e.g. via Jailbreak or Root), we reserve the right to terminate your access to Online Banking which will include your access to HSBC's mobile banking app.

Users agree not to interfere with or damage (or attempt to interfere with or damage) any PBN, PIN, Username, Password, Security Code, Secure Key, data or software associated with the Online Banking Service.

The security guidelines in this clause provide examples only and will not determine your liability for any losses arising from unauthorised EFT transactions.

Liability for unauthorised EFT transactions will be determined in accordance with Clause 6 of these Terms and ePayments Code rather than these guidelines.

2.7 Recording Telephone Calls

HSBC may record telephone calls made to HSBC's Direct Service Centre for training, verification, authentication and quality control purposes.

2.8 Bill payments - BPAY® Scheme

The provisions under this heading of "Bill payments BPAY® Scheme" apply if and when HSBC is instructed to make a BPAY® payment using the Service. These provisions operate in conjunction with these Terms as well as the terms and conditions applicable to EFT Accounts accessed using the Online Banking Service. If there is any inconsistency between the terms and conditions applying to the EFT Account to be debited and the provisions set out under this heading, these provisions prevail to the extent of the inconsistency.

(a) BPAY® payment instructions

The following information must be given to HSBC to instruct it to make a BPAY® Payment:

(i) the Username and Password;

(ii) where requested by HSBC the Security Code (e.g. if a Secure Key has been issued to the User);

(iii) the EFT Account from which the payment is to be made;

(iv) the amount to be paid;

(v) the Biller's code number (found on the bill); and

(vi) the Customer Reference Number (e.g. the account number with the Biller).

HSBC will then debit your EFT Account with the amount of that BPAY® Payment. HSBC will not be obliged to effect a BPAY® Payment Instruction if the information given is incomplete and/or inaccurate.

(b) Processing Payments

Generally, a BPAY® Payment will be treated as received by the Biller to whom it is directed:

- on the date HSBC is told to make it, if this occurs before the Payment Cut-off Time on a Banking Day; or
- otherwise, on the next Banking Day.

A delay might occur in the processing of a BPAY® Payment where:

- there is a public or bank holiday on the day after HSBC is told to make a BPAY® Payment; or
- a Biller, or another financial institution participating in the BPAY® Scheme, does not comply with its obligations under the BPAY® Scheme.

While it is expected that any delay in processing a payment for any of these reasons will not continue for more than one Banking Day, any such delay may continue for a longer period. It is the User's responsibility to allow for sufficient time for processing of payments to the Biller.

Users must be careful to tell HSBC the correct amount to be paid. If the amount HSBC was instructed to pay was less than the amount needed to be paid, another BPAY® Payment should be made for the shortfall. If the amount HSBC was instructed to pay was greater than the amount intended, the Biller should be contacted to obtain a refund.

HSBC will attempt to make sure that BPAY® Payments are processed promptly by Billers and other participants in the BPAY® Scheme.

HSBC will not accept an instruction to stop a BPAY® Payment once it has been instructed to make that BPAY® Payment.

If HSBC is advised by a Biller that a BPAY® Payment cannot be processed, HSBC will:

- advise you of this;
- credit the relevant EFT Account with the amount of that BPAY® Payment; and
- take all reasonable steps to assist in making the BPAY® Payment as quickly as possible.

(c) Liability for unauthorised, fraudulent or mistaken BPAY®

payments

A mistaken BPAY® Payment is a BPAY® Payment to a person or for an amount which is not in accordance with the Instructions given to HSBC, if any. If your EFT Account is debited with the amount of a mistaken BPAY® Payment, HSBC will credit that amount to your EFT Account. However, you must pay HSBC the amount of a mistaken BPAY® Payment if a User is responsible for a mistake resulting in that payment and HSBC cannot recover the amount from the person who received it within 20 Banking Days of attempting to do so.

You acknowledge that the receipt by a Biller of a mistaken or erroneous payment does not or will not constitute under any circumstances part or whole satisfaction of any underlying debt owed between you and that Biller.

If you notify HSBC that a BPAY® Payment made from your EFT Account is Unauthorised, you must provide HSBC with a written consent addressed to the Biller who received that BPAY® Payment, allowing HSBC to obtain from that Biller information about your account with that Biller or the BPAY® Payment, including your customer reference number and such information as is reasonably required to investigate the BPAY® Payment. If you do not give that consent to HSBC, the Biller may not be permitted under law to disclose to HSBC the information it needs to investigate or rectify that BPAY® Payment.

(d) Consequential damage and indemnity

Subject to the Terms and the ePayments Code:

(a) HSBC is not liable for any consequential loss or damage you may suffer as a result of using the BPAY® Scheme, other than due to any loss or damage you suffer due to the negligence of HSBC, or in relation to any breach of a condition or warranty implied by law in contracts for the supply of goods and services and which may not be excluded, restricted or modified at all or only to a limited extent; and

(b) you indemnify HSBC against any loss or damage it may suffer due to any claim, demand or action of any kind brought against it arising directly or indirectly because you:

(i) did not observe any of your obligations under; or

(ii) acted negligently or fraudulently in connection with, these Terms.

(e) Suspension

HSBC may at any time suspend your right to participate in the BPAY® Scheme and will do so without notice if HSBC suspects a User, or someone acting on your behalf, of

being fraudulent. BPAY® Payments for which Instructions have been given and which are scheduled to be made while your right to participate in the BPAY® Scheme is suspended will not be processed by HSBC.

3. SECURITY OF ACCESS METHODS

3.1 Protecting Access Methods

Users must keep their Access Methods secure to prevent Unauthorised use of EFT Accounts. Users must take care to ensure that Access Methods and the Secure Key (if supplied) are not misused, lost or stolen and that the PIN, Password and the Security Code does not become known to anyone else.

3.2 Guidelines

3.2.1 These guidelines should be followed by Users to ensure the security of an Access Method. These guidelines are examples only and will not determine your liability for any losses resulting from unauthorised EFT transactions on your Account. Liability for such transactions will be determined in accordance with Part 6 below and the ePayments Code.

3.2.2 **To protect the PIN and Password:**

(a) Memorise the PIN when it is received and destroy HSBC's notification of the PIN.

(b) Memorise the Password.

(c) Do not tell or show the PIN or Password to another person or allow it to be seen by another person (including family and friends).

(d) Do not keep a record of a PIN or Password in a way in which it can be determined by another person.

(e) Do not record a PIN or Password and Identifier together, or record a PIN or Password on the Secure Key.

(f) Do not record a PIN or Password on anything which is kept with or near a Secure Key without making a reasonable attempt to disguise the PIN or Password or prevent Unauthorised access to the record.

(g) Do not record the PIN or Password on Electronic Equipment or related articles without making a reasonable attempt to disguise the PIN or Password or prevent Unauthorised access to the record.

(h) Keep the PIN and Password separate from the Secure Key, and never where they can both be found together, for example in a wallet, handbag, desk, document, file, briefcase, bedroom dresser, locker, car or clothing.

(i) Do not allow anyone to watch the PIN or Password being

entered at Electronic Equipment.

3.2.3 **Notification**

Notify HSBC immediately by telephoning 1300 306 543 at any time if a record of a PIN or Password is lost or stolen or if a User suspects that someone else may know a PIN or Password.

3.2.4 **Memory aids and reasonable disguises**

If a memory aid is required to recall the PIN or Password such a record may be made provided the record is reasonably disguised.

Examples which we do not consider provide a reasonable disguise are:

(a) recording the PIN or Password as a series of numbers with any of them marked, circled or highlighted to indicate the PIN or Password;

(b) recording the PIN or Password with surrounding information which makes it stand out from its context;

(c) recording the PIN or Password as a string of digits in isolation from other information unless the context provides adequate disguise;

(d) disguising the PIN or Password by reversing the number sequence;

(e) describing the disguised record as a "PIN record" or "Password record" or similar;

(f) disguising the PIN or Password using alphabetical characters or numbers eg A=1, B=2, C=3, etc, or in any other easily understood code;

(g) selecting or disguising the PIN or Password using any of the following combinations (or parts of them), with the PIN or Password in its correct sequence within the combination:

  (i) dates of birth;

  (ii) personal telephone numbers;

  (iii) car registration numbers;

  (iv) family members' names;

  (v) social security numbers; or

  (vi) licence numbers.

(h) recording the PIN or Password as a:

  (i) date of birth;

  (ii) postcode; or

  (iii) telephone number, without additional features of disguise;

(i) storing the PIN or Password in any low security electronic device of any kind, such as (but not limited to):

  (i) calculators;

  (ii) personal computers; or

  (iii) electronic organisers.

There may be other forms of disguise which may also be unsuitable because of the ease of another person discerning the PIN or Password.

3.2.5 **To protect the Security Code**

(a) Carry the Secure Key whenever possible.

(b) Always keep the Secure Key in a safe place and check regularly to ensure that it has not been lost or stolen.

(c) Do not record a PIN or Password or an Identifier on the Secure Key.

(d) Do not record a PIN or Password or an Identifier on anything which is kept with or near a Secure Key without making a reasonable attempt to disguise the PIN or Password or Identifier.

(e) Do not lend the Secure Key to anyone.

(f) Do not tell or show the Security Code to another person or allow it to be seen by another person (including family and friends).

(g) Do not leave the Secure Key behind after making an EFT Transaction.

(h) Do not drop the Secure Key or expose it to high heat, liquids or attempt to disassemble the Secure Key.

Notify HSBC immediately by telephoning 1300 306 543 at any time if the Secure Key is misused, lost or stolen.

4. REPORTING LOSS, THEFT OR UNAUTHORISED USE OR BREACH OF PIN, SECURE KEY OR SECURITY CODE SECURITY OR MISTAKEN INTERNET PAYMENTS ETC

Users must notify HSBC immediately if a PIN or Password or Security Code becomes known to someone else, if a Secure Key is misused lost or stolen or if a transaction is suspected to have been made on an EFT Account without a User's authority.

Users should also notify HSBC if they believe they have made a mistake in instructing HSBC to make a BPAY® Payment, if there are any delays or mistakes in processing BPAY® Payments, if a BPAY® Payment that has been made from an EFT Account is Unauthorised, or if a User has been fraudulently induced to make a BPAY® Payment.

Users should also notify HSBC immediately if they believe they have made a Mistaken Internet Payment.

Users should notify HSBC in Australia by calling us on 1300 306 543. If overseas, Users should report to any branch of a Group member bank or call +612 9005 8187.

HSBC may cancel the Access Method (involving, if relevant, deactivating the Secure Key), and arrange for the User to select or be provided with a new one, as appropriate.

HSBC will acknowledge the notification by giving the User a reference number that verifies the date and time HSBC was contacted. The number is proof that HSBC was advised according to these Terms and should be kept for future reference.

If for any reason HSBC's hotline is unavailable and this prevents notification, you will not be liable for any Unauthorised transaction which could have been prevented during this period if the hotline had been available, provided HSBC is notified within a reasonable time of the hotline becoming available again.

You agree that HSBC may disclose information about you or your EFT Account to the police or other third parties if it thinks it will help prevent or recover losses or if it is legally obliged to do so.

5. MISTAKEN INTERNET PAYMENTS

5.1 ADIs must investigate

Where a User reports a Mistaken Internet Payment, HSBC will investigate whether a Mistaken Internet Payment has occurred.

If HSBC is satisfied that a Mistaken Internet Payment has occurred, HSBC will send the Receiving ADI a request for return of the funds.

If HSBC is not satisfied that a Mistaken Internet Payment has occurred, HSBC will not take any further action.

5.2 Process where funds are available and report is made within 10 business days

Where a User reports a Mistaken Internet Payment within 10 business days of making the payment and:

(a) HSBC and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred; and

(b) HSBC is advised by the Receiving ADI that there are sufficient credit funds available in the account of the Unintended Recipient to the value of the Mistaken Internet Payment, the Receiving ADI must forward the funds to HSBC no later than 10 business days after receiving our request to return the funds.

5.3 Process where funds are available and report is made between 10 business days and seven months

Where a User reports a Mistaken Internet Payment between 10 business days and seven months after making the payment and:

(a) HSBC and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred; and

(b) HSBC is advised by the Receiving ADI that there are sufficient credit funds available in the account of the Unintended Recipient to the value of the Mistaken Internet Payment,

The Receiving ADI must:

(a) prevent the Unintended Recipient from withdrawing the funds for 10 further business days; and

(b) if the Unintended Recipient does not establish that they are entitled to the funds during this period, the Receiving ADI must return the funds to HSBC within two business days after the expiry of the 10 business day period referred to above.

5.4 Process where funds are available and report is made after seven months

Where a User reports a Mistaken Internet Payment more than seven months after making the payment and:

(a) HSBC and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred;

(b) HSBC is advised by the Receiving ADI that there are sufficient credit funds available in the account of the Unintended Recipient to the value of the Mistaken Internet Payment; and

(c) the Unintended Recipient consents to return of the funds,

the Receiving ADI must forward the funds to HSBC.

5.5 Process where funds are not available

Where HSBC and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred, but there are insufficient credit funds available in the account of the Unintended Recipient to the full value of the Mistaken Internet Payment, the Receiving ADI must use reasonable endeavours to retrieve the funds from the Unintended Recipient for return to the holder.

If the Receiving ADI is unable to recover the funds from the Unintended Recipient, the account holder will be liable for losses arising from the Mistaken Internet Payment.

5.6 Unintended Recipient

If you receive a Mistaken Internet Payment into your account, you authorise HSBC, as Receiving ADI, to withdraw the funds from your account and return the funds to the Sending ADI in order to comply with our obligations under the ePayments Code.

6. LIABILITY FOR UNAUTHORISED EFT TRANSACTIONS

6.1 Authorised transaction

You are liable for all EFT Transactions carried out in respect of your EFT Accounts with the knowledge and consent of a User.

6.2 When you are not liable

You will not be liable for losses in respect of an EFT Account caused by an Unauthorised EFT Transaction:

(a) resulting from Unauthorised use of a PIN, or Security Code before the User has received the PIN or

Secure Key which forms part of their Access Method;

(b) after HSBC receives notification that a PIN, Password or Secure Key has been misused, lost, stolen or the PIN, Password or Security Code has become known to someone else;

(c) relating to any component of an Access Method that is forged, faulty, expired or cancelled;

(d) caused by the fraudulent or negligent conduct of employees or agents of:

(i) HSBC; or

(ii) any organisation involved in the provision of the EFT System

(e) where it is clear that the User has not contributed to the loss;

(f) caused by the same transaction being incorrectly debited more than once to the same EFT Account; or

(g) where the transaction can be made using an account number without a PIN, Password, Security Code or Secure Key. Where a transaction can be made using a Secure Key, or a Secure Key and an account number, but does not require a PIN, Password or Security Code,
you will be liable only if the User unreasonably delays reporting the loss or theft of the Secure Key.

6.3 When you are liable

6.3.1 Where HSBC proves on the balance of probabilities that the User has contributed to the losses in respect of an EFT Account resulting from an Unauthorised EFT Transaction by:

(a) the User's fraud;

(b) (where the User has not been issued with a Secure Key) voluntarily disclosing the PIN, or Password to anyone, including a family member or friend;

(c) (where the User has been issued with a Secure Key) voluntarily disclosing the PIN, or Password and showing the Secure Key or otherwise disclosing the Security Code to anyone, including a family member or friend;

(d) (where the User has been issued with a Secure Key) voluntarily disclosing the PIN, or Password or showing the Secure Key (or otherwise disclosing the Security Code), but not all (PIN/Password and Secure Key), to anyone, including a family member or friend, where this disclosure is more than 50% responsible for the losses when all other contributing causes are assessed together;

(e) where the Access Method comprises the PIN and PBN or Username and Password only,

keeping a record of the PIN or Username and/or Password on one article or on several articles so that they are liable to loss or theft simultaneously, without making any reasonable attempt to disguise the PIN and PBN or Username or Password or taking reasonable steps to prevent Unauthorised access to that record;

(f) where the Access Method comprises a PIN, PBN or Username and Password and Security Code, keeping a record of the PIN and PBN or Username and/or Password on one or more articles liable to loss or theft simultaneously and keeping the Secure Key (without making any reasonable attempt to protect the security of the record of the PIN, Username, Password or Secure Key) so that they are liable to loss or theft simultaneously;

(g) where the Access Method comprises a PIN and PBN, Username and Password and Security Code, keeping a record of the PIN and PBN, Username and/or Password (on one or more articles liable to loss or theft simultaneously) or keeping the Secure Key (without making any reasonable attempt to protect the security of the record of the PIN and PBN or Username, Password or Secure Key), but not all, so that they are liable to loss or theft, where doing so is more than 50% responsible for the losses when all other contributing factors are assessed together;

(h) when selecting or changing a PIN, Username and/or Password, choosing a PIN, Username and/or Password which represents as a numeric code the User's birth date or an alphabetical code which is a recognisable part of the User's name; or

(i) acting with extreme carelessness in failing to protect the security of the PIN, Username, Password or Security Code,

you will be liable for the losses which occur before HSBC is notified of the loss or theft of the Secure Key, unauthorised use or breach of PIN, Username, Password or Security Code security.

6.3.2 Where more than one PIN, Password or Security Code is required to perform a transaction and HSBC proves that a User breached the security requirements in clause 3 for one or more, but not all, of the required PINs, Passwords or Security Codes, you are liable under clause 6.3 only if HSBC also proves on the balance of probability that the breach of the security requirements in clause 3 was

more than 50% responsible for the losses, when assessed together with all the contributing causes.

6.3.3 Where HSBC proves on the balance of probabilities that the User has contributed to losses in respect of an EFT Account resulting from an Unauthorised EFT Transaction by unreasonably delaying in notifying HSBC of the Unauthorised use, loss or theft of the Secure Key or that the PIN, Username, Password or Security Code has become known to someone else, you will be liable for the losses which occur between when the User became aware of the loss, theft or Unauthorised use or that the PIN, Username, Password or Security Code became known to someone else and when HSBC was actually notified.

6.3.4 However, even if we prove on the balance of probabilities that the User has contributed to losses, you will not be liable for:

(a) that portion of the loss incurred on any one day which exceeds any applicable daily transaction limits;

(b) that portion of the loss incurred in a period which exceeds any other periodic transaction limits applicable to that period;

(c) that portion of the loss on your EFT Account which exceeds the balance of your EFT Account, including any pre-arranged credit; or

(d) that portion of the loss incurred on any account that HSBC and the account holder had not agreed could be accessed using the Secure Key and/or PIN, Password or Security Code used to perform the transaction.

6.4 When your liability is limited

Where a PIN, Password or Security Code was required to perform the unauthorised EFT transaction and we do not prove that you have contributed to losses, your liability for any loss in respect of an EFT Account arising from an unauthorised EFT transaction is the lesser of:

(a) $150.00, or a lower figure determined by HSBC;

(b) the balance of the EFT Account (or where you have pre-arranged credit the approved credit limit), but only if you had agreed with HSBC that the EFT Account could be accessed with the Access Method; or

(c) the actual loss at the time HSBC is notified of the unauthorised use, loss or theft of the Secure Key or the breach of PIN, Password or Security Code security (except that portion of the loss incurred on any one day

that exceeds any daily or periodic transaction limits applicable to the use of the Access Method or EFT Account).

6.5 Electronic system malfunctions

If the system provided by, or on behalf of, HSBC to facilitate EFT Transactions malfunctions, HSBC will account to you for any loss caused by the system accepting a User's Instructions but failing to complete the transaction. However, if the User should have known that the system was unavailable for use or malfunctioning, HSBC will only be responsible for correcting errors in the EFT Account and refunding to you any associated fees or charges. Users should make a note of the time of the malfunction and the amount involved and report the malfunction to HSBC.

You should also check your next EFT Account statement to verify that the necessary corrections have been made to the EFT Account.

7. PROCEDURES FOR HANDLING ERRORS AND INVESTIGATING AND RESOLVING COMPLAINTS

7.1 How to lodge a complaint

If you believe an EFT Transaction is wrong or Unauthorised, or there is an error in an EFT Account statement, or where HSBC is the Sending ADI and you wish to make a complaint regarding a Mistaken Internet Payment, or if you otherwise have any concerns about a procedure, compliance issue, or have encountered a problem with our service, we want you to tell us about it. We have designed a simple customer complaint process.

If you are a customer and have a complaint or concern, make it known at your branch where the Branch Customer Service Manager should be able to resolve the problem; if not, the Branch Manager can undertake further investigation and action.

7.2 Customer Relations

If your complaint hasn't been resolved to your satisfaction, contact our Customer Relations Complaints team:

Toll Free: 1300 308 188
Facsimile: 02 9006 5130
Mail:
Customer Relations Department,
HSBC Bank Australia Limited,
Level 36, Tower 1 - International Towers Sydney
100 Barangaroo Avenue
Sydney NSW 2000
Australia

Or you can log onto our website, www.hsbc.com.au and record your complaints or feedback via the "Contact Us" icon.

7.3 HSBC's investigations

HSBC will try to resolve your query as soon as possible, however some problems are complicated and may take time to resolve.

If HSBC is unable to resolve your

complaint immediately to your satisfaction, HSBC will advise you of the procedures for the further investigation and handling of your complaint and may ask you to provide further details. For example, if there is a dispute over who is liable for a loss resulting from an unauthorised transaction, you will be asked to complete and sign a form providing further information. HSBC will investigate your complaint and within 21 days of receiving your complaint write to you, explaining the outcome of its investigation or that more time is needed to complete the investigation.

Unless there are exceptional circumstances, HSBC will complete its investigation within 45 days of receiving your complaint. If HSBC is unable to resolve your complaint within 45 days, HSBC will write to you and inform you of the reasons for the delay and provide you with monthly updates on the progress of its investigation and an indication of when your complaint is likely to be resolved, except where HSBC is awaiting a response from you and you have been advised that it requires such a response.

7.4 Results of HSBC's investigation

When HSBC completes its investigations of your complaint, it will notify you in writing of:

(a) the result;

(b) the reasons for its decision with reference to the relevant provisions of the Terms and ePayments Code; and

(c) any further action you can take in respect of your complaint.

If your EFT Account is found to have been incorrectly credited or debited, HSBC will adjust your EFT Account accordingly (including any interest and charges) and notify you in writing of the amount of the adjustment and, if the incorrect crediting relates to a discrepancy between the amount recorded by the Electronic Equipment or Access Method as having been deposited and the amount recorded by us as having been received, we will also notify you of the difference and the actual amount which has been credited to your EFT Account.

If HSBC finds that you are liable for all or part of the disputed transaction, it will supply you with copies of any document or other evidence on which it based its findings, and advise you in writing, if there was any system or equipment malfunction at the time of the transaction.

If you are not satisfied with the decision, you may wish to take the matter further. You may, for instance, contact the Financial Ombudsman Service.

Where HSBC is the Receiving ADI in a Mistaken Internet Payment dispute, you agree that you may be

subject to the Sending ADI's external dispute resolution scheme, including complying with any decision of that scheme.

7.5 Financial Ombudsman Service

The Financial Ombudsman Service (FOS) scheme is an impartial, independent and free service for personal and small business customers.

The FOS cannot investigate:

(a) A claim for more than $500,000.

(b) A claim in relation to a commercial decision by HSBC, such as whether a loan is approved.

(c) A claim in relation to HSBC's general policy or practice, such as interest rates or fees.

For more information refer to the FOS website www.fos.org.au

You can contact the FOS by writing to:
Financial Ombudsman Service
GPO Box 3, Melbourne, VIC 3001

Phone: 1300 780 808
Facsimile: (03) 9613 6399
Email: info@fos.org.au

7.6 If HSBC does not comply with these procedures

HSBC may be liable for part or all of the amount of the disputed transaction if:

- HSBC fails to comply with the appropriate procedures for handling complaints, allocating liability or communicating the reasons for its decision; and
- that failure contributes to HSBC's decision or delays the resolution of your complaint.

8. HSBC Mobile Banking App

8.1 These Terms and Conditions (these "Terms") apply to the HSBC mobile banking app together with:

- the terms and conditions that apply to any account or service you can access using the HSBC mobile banking app (the "Product Terms"); and
- our Terms and Conditions for Online Banking ("Online Banking Terms") which are incorporated in these Terms by reference; and
- any other terms and conditions that we may notify you.

In the event of a conflict between these Terms and the Product Terms or the Online Banking Terms, these Terms will prevail.

Terms and expressions used in these Terms shall have the same respective meanings as defined in the Online Banking Terms unless the context requires otherwise.

8.2 The HSBC mobile banking app allows you to access some of our Online Banking Services in a format which is easier to view on a mobile device.

8.3 You can log on to the HSBC mobile banking app by:

- using your Access Method for Online Banking;
- entering a Digital Secure Key password. You can set up a Digital Secure Key on any mobile device that supports this functionality with such operating system version as we specify from time to time;
- using your Access Method as we request and a Security Code generated by a Secure Key or a Digital Secure Key set up on another mobile device; or
- activating biometric credentials (e.g. fingerprint, facial map or any other biometric data) that we may enable for use in the HSBC mobile banking app (and any other mobile applications that we may support from time to time (for compatible devices only)) for authentication purpose. In order to enable this functionality, your compatible device must support the receiving of the relevant biometric credentials, have the HSBC mobile banking app downloaded to it and have the relevant biometric authentication methods enabled for use in the HSBC mobile banking app.

You may be required to perform one or more of the above in order to access full services of the HSBC mobile banking app.

8.4. Using the HSBC mobile banking app

8.4.1 The HSBC mobile banking app can be used on a mobile device running an operating system supported and specified by us from time to time, from which you can access the internet. However, not all of our services available on Online Banking can be accessed using the HSBC mobile banking app.

8.4.2 You can set up a Digital Secure Key within the HSBC mobile banking app on any device that supports this functionality. But you can only set up a Digital Secure Key on one mobile device at a time. You can use the Digital Secure Key to log into Online Banking and also the HSBC mobile banking app.

8.4.3 Updates to the HSBC mobile banking app may be issued periodically through the supplying app store. For some devices, updates will be downloaded automatically. If this does not happen, you will need to download the update yourself. We may display in-App messages when you try to log on to remind you to do this. You should log on to the HSBC mobile banking app regularly to check these messages. Depending on the update, you may not be able to use the HSBC mobile banking app until the latest version has been

downloaded. If the latest version of the HSBC mobile banking app has not been downloaded and you have set up a Digital Security Key, you may also not be able to access Online Banking. To make sure you always have access to the HSBC mobile banking app and Online Banking, you should keep your HSBC mobile banking app updated.

8.4.4 The HSBC mobile banking app may only be installed and used by our customers. It is not intended for download, or use by, any person who is not already our customer or in any jurisdiction where such download or use would be contrary to any law or regulation of such jurisdiction or where we are not licensed or authorised to provide the HSBC mobile banking app or the related services.

8.4.5 We do not charge for the HSBC mobile banking app. However, your mobile network operator may charge you to download or access the HSBC mobile banking app and its features including the Digital Secure Key and these charges may vary if you download or access the HSBC mobile banking app when abroad. You are responsible for these charges.

8.4.6 Certain services, including the Find a Branch/ATM and Offers and Rewards, use information about your physical location sent from your mobile device (for example, GPS signals). If you use these services, you consent to us, our partners and licensees, and Google accessing, monitoring, transmitting, collecting, maintaining, disclosing, processing and using your location data to enable us and Google to provide the relevant functionality in accordance with the terms and conditions, and privacy policy, of the HSBC mobile banking app and those of Google. You will be asked to consent to the use of location services when you download the HSBC mobile banking app or the first time you use the relevant services. You may withdraw this consent at any time by turning off the location services settings on your mobile device.

8.4.7 Access to third party services (such as Google Maps/Google Earth API) through the HSBC mobile banking app is subject to separate terms and conditions of third party service providers (such as Google terms and conditions available at http://maps.google.com/help/terms_maps.html and http://www.google.com/enterprise/earthmaps/legal/universal_aup.html).

8.4.8 iPhone, iPad, iPod Touch, Touch ID, Face ID and Apple are trademarks of Apple Inc., registered in the US and other countries. App Store is a service mark of Apple Inc. Google Play™ is a trademark of Google Inc. Android™ is a trademark of Google Inc.

8.5. Your Responsibilities

8.5.1 You must comply with all applicable laws and regulations that govern your download, access and use of the HSBC mobile banking app and Digital Secure Key.

8.5.2 You must not alter, modify, adapt, reverse-engineer, copy or reproduce all or any part of the HSBC mobile banking app.

8.5.3 You must not remove or tamper with any copyright notice attached to or contained within the HSBC mobile banking app. All ownership in the HSBC mobile banking app remains with us.

8.5.4 The HSBC mobile banking app is for your personal use only, and you must not use the HSBC mobile banking app for business or commercial or other unauthorised purposes.

8.5.5 You must take security measures on your mobile device as recommended by HSBC from time to time, otherwise, to the extent permitted under the ePayments Code or any law, you will bear the associated risks and consequences which may arise from or in connection with your mobile device and the use of the HSBC mobile banking app.

8.6. Our Responsibilities

8.6.1 While we make reasonable efforts to provide the HSBC mobile banking app services including the Digital Secure Key feature, we will not be liable for any failure to provide those services, in part or in full, due to abnormal and unforeseen circumstances beyond our control, the consequences of which would have been unavoidable despite all efforts to the contrary. This includes any phone network failures or, in the case of mobile networks, where you are not in an area of mobile coverage.

8.6.2 The HSBC mobile banking app and the Digital Secure Key feature is provided "as is" with no representation, guarantee or agreement of any kind as to its functionality. We cannot guarantee that no viruses or other contaminating or destructive properties will be transmitted or that no damage will occur to your mobile device. We are not responsible for any loss you may incur as a result of this.

8.7. Security

8.7.1 You must take all reasonable precautions to keep safe and prevent fraudulent use of your mobile device and security information. These precautions include:

- 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 it;
- keeping your security details unique to Online Banking and the HSBC mobile banking app;
- ensuring that your biometric credentials stored on your device are your own and do not store anyone else's biometric credentials on your device and that you only use your own biometric credentials to log on to the HSBC mobile banking app (and any other mobile applications that we may support from time to time (for compatible devices only));
- not using facial recognition for authentication purpose if you have an identical twin sibling, in which case you are recommended instead to use the Digital Secure Key password to generate the Security Code or to log on to the HSBC mobile banking app (and any other mobile applications that we may support from time to time (for compatible devices only));
- not using facial recognition for authentication purpose if you are an adolescence while your facial features may be undergoing a rapid stage of development, in which case you are recommended to instead use the Digital Secure Key password to generate the Security Code or log on to the HSBC mobile banking app (and any other mobile applications that we may support from time to time (for compatible devices only));
- not taking any action to disable any function provided by, and/or agreeing to any settings of, your mobile device that would otherwise compromise the security of the use of your biometric credentials for authentication purposes (e.g. disabling "attention-aware" for facial recognition);
- 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;
- once you have logged on to the HSBC mobile banking app do not leave your mobile device unattended or let anyone else use your mobile device;
- logging out of the HSBC mobile

banking app once you have finished using the HSBC mobile banking app services, and in particular not leaving the HSBC mobile banking app running in the background whilst logged in (for example, whilst multi-tasking, or running other apps);

- follow all security measures provided to you by the manufacturer of your mobile device operating system that apply to your use of the HSBC mobile banking app or your mobile device (although you should never disclose your security details to them or information about your accounts with us); and
- undertake reasonable and adequate precautions to scan for computer viruses or other destructive properties.

8.7.2 You must not use the HSBC mobile banking app and the Digital Secure Key feature 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 "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 HSBC mobile banking app and the Digital Secure Key feature on a jail broken or rooted device may compromise security and lead to fraudulent transactions. Download and use of the HSBC mobile banking app and the Digital Secure Key feature in a jail broken or rooted device is entirely at your own risk and HSBC will not be liable for any losses or any other consequences suffered or incurred by you as a result.

8.7.3 You should only download the HSBC mobile banking app and its updates from official supplying app store and not from any unofficial sources.

8.7.4 We will 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 any such request from anyone (even if they are using our name and logo and appear to be genuine) then it is likely to be fraudulent and you must not supply your security details to them in any circumstances. Additionally, you should report any such requests to us immediately.

8.7.5 You will be responsible for all instructions given by you or anyone acting with your authority between when you log on to the HSBC mobile banking app until you log off the HSBC mobile banking app.

8.7.6 You are responsible for making sure information shown or stored on your mobile device is kept secure.

8.7.7 You must advise us of any change to your mobile phone number without delay.

8.7.8 If you activate the feature that allows you to use your biometric credentials in the HSBC mobile banking app and to enable the use of such biometric credentials to log on to the HSBC mobile banking app (and any other mobile applications that we may support from time to time (for compatible devices only)), you must ensure that only your biometric credentials are registered on the device.

8.7.9 To the extent permitted by the ePayments Code or any law, you may be responsible for unauthorised payments made from your accounts if you have not kept your mobile device and your security details safe and follow the security precautions that we advise you to undertake from time to time including those set out in this Clause 8, or if the biometric credentials stored on your device are not your own in the event that you have activated such authentication method on the device and on the HSBC mobile banking app.

8.7.10 If you know or suspect that someone else knows your security details, or has used or tried to use them, or if your mobile device is lost or stolen you must tell us without delay by calling us on such number as we specify from time to time.

8.7.11 Upon termination of the HSBC mobile banking app services for any reason, you must remove the HSBC mobile banking app from your mobile device.

8.7.12 You must delete the HSBC mobile banking app from your mobile device if you change your mobile device or dispose of it.

8.7.13 If the HSBC mobile banking app has been terminated or suspended for any reason, and if Online Banking is still available to you, you will need to apply to us for a new Secure Key in order to continue accessing full services of Online Banking.

PART B

Supplementary Product Disclosure Statement
for HSBC Online Banking

IMPORTANT INFORMATION

This Supplementary Product Disclosure Statement (**"SPDS"**) supplements, and is intended to be read with, the HSBC Online Banking Product Disclosure Statement to which it is appended (see Part A).

The date of this SPDS is 1 August 2017.

This SPDS only applies to HSBC Premier Customers. It does not apply to, and need not be read by, a customer who is not an HSBC Premier Customer. For HSBC Premier Customers, this SPDS provides information on, and includes the Terms and Conditions for Global Transfers, which can be made in connection with Global View, another service which is only available to HSBC Premier Customers.

This SPDS is intended to operate in conjunction with the PDS. However, if there is any inconsistency, the SPDS prevails in respect of Global Transfers.

Issuer details

This SPDS is issued by HSBC Bank Australia Limited (ABN 48 006 434 162) (AFSL 232 595).

GLOBAL TRANSFERS TERMS AND CONDITIONS

1. Definitions

Where relevant, terms defined in the PDS apply to the SPDS. In addition, the following terms have the following meaning in the SPDS:

"Banking Day" means:

- for a Global Transfers Supported Currency, any day on which The Hongkong and Shanghai Banking Corporation Limited's Hong Kong Treasury department is open for trading; and
- for a Global Transfers Unsupported Currency, any day on which one or more branches of the Group are open for business in the country with which HSBC needs to communicate to effect or arrange a Global Transfer or other transaction.

"Currency Conversion" means an exchange of one currency for another at an exchange rate determined, in the case of a Global Transfers Supported Currency, by The Hongkong and Shanghai Banking Corporation Limited's Hong Kong Treasury department or, in the case of a Global Transfers Unsupported Currency, by the Group member with which you hold the account to which the Global Transfer is to be made.

"Global Transfer" means an electronic transfer of currency from an account held by an HSBC Premier Customer with one member of the Group to an account held by that same customer with another member of the Group. Both accounts must be linked to, and be able to be viewed using, Global View.

"Global View" means the service marketed under the name "HSBC Premier Global View" which is made available as part of the Online Banking Service to HSBC Premier Customers only and on separate terms and conditions ("Global View Terms and Conditions"). Global View enables customers of members of the Group to link to, and view on, any Group member's internet website their accounts held with a Group member which are accessible through Online Banking.

"HSBC Premier" means the service and product proposition marketed under that name and made available to HSBC Premier Customers.

"HSBC Premier Customer" means a customer who satisfies the eligibility criteria set by HSBC from time to time for HSBC Premier Customer status and who, in HSBC's discretion, is given that status.

"Global Transfers Supported Currency" means a currency offered by The Hongkong and Shanghai Banking Corporation Limited's Hong Kong Treasury department for the purpose of Global Transfers and in respect of which The Hong Kong Treasury department will undertake the settlement of a Currency Conversion where a Currency Conversion is required.

"Global Transfers Unsupported Currency" means a currency which HSBC advises can be the subject of a Global Transfer, but is not a currency offered by The Hongkong and Shanghai Banking Corporation Limited's Hong Kong Treasury department for the purpose of Global Transfers. If a Currency Conversion to such a currency is required it will be undertaken by the Group member with which you hold the account to which the Global Transfer is to be made.

"USD" means United States Dollar.

"24 Hour Period" means the period of time between 00.00hrs GMT and 2400hrs GMT.

2. About these Terms and Conditions

These Terms and Conditions operate together with the terms in the PDS. If there is an inconsistency between these Terms and Conditions and the terms in the PDS, these Terms and Conditions prevail in respect of Global Transfers.

For the avoidance of doubt, the definition of "Terms" in clause 1.1 of the PDS is to be read as including the Global Transfer Terms and Conditions.

3. Acceptance

You agree to these Global Transfer Terms and Conditions when, having been presented with these Terms and Conditions on our website (www.hsbc.com.au) as part of the Combined Product Disclosure Statement and Supplementary Product Disclosure Statement, a User clicks the "Accept" button indicating acceptance of the Terms and Conditions.

4. Entitlement to make Global Transfers

You can only access the service which allows a Global Transfer to be made if:

(a) you have access to the Online Banking Service;

(b) you are an HSBC Premier Customer;

(c) you have access to Global View, and have agreed to the Global View Terms and Conditions; and

(d) you have accepted these Global Transfers Terms and Conditions.

5. Global Transfer requirements

Subject to these Terms and Conditions and the terms and conditions applying to the accounts to be the subject of the Global Transfer, you may effect a Global Transfer from an EFT Account to an account you have with another Group member provided that:

- both accounts are linked in, and can be viewed using, Global View;
- you have a sufficient available balance in the EFT Account; and
- the amount to be transferred is within the Agreed Limits (see clause 8).

The Global Transfer may be made either in the same currency in which funds are held in the EFT Account or in a different currency provided that the account to which the transfer is required to be made is an account in the same currency as that selected by you for the transfer. A Currency Conversion will apply if a different currency is to be transferred. For instance if you have accounts in Canadian Dollars (CAD) in Australia and also with the HSBC Group in Canada, you can instruct the transfer to be in CAD and there will be no Currency Conversion. Alternatively if you have an account in Australian Dollars (AUD) in Australia and in CAD in Canada, you can instruct the transfer to be in CAD and, in that case, a Currency Conversion will be required.

6. Global Transfers Supported Currencies – Instruction times and exchange rates

This clause applies to an Instruction to effect a Global Transfer in a Global Transfers Supported Currency.

If you give an Instruction to us on a Banking Day and request that it be processed immediately, the Instruction will be processed on the same Banking Day if we receive the Instruction prior to 2400 hrs GMT. If a Currency Conversion is required, the currency exchange rate that will be applied is the rate that applies at the time you give the Instruction. The applicable rate will be advised to you before the transfer is processed.

If you give an Instruction to make a Global Transfer:

- on a future Banking Day; or
- at any time on a day that is not a Banking Day,

the Instruction will be processed on the requested future Banking Day or the next Banking Day (as relevant) and, in each case, if a Currency Conversion is required, at the currency exchange rate that applies at the time the Instruction is processed.

Please note that due to fluctuations in currency exchange rates, if we are provided with Instructions to effect a Global Transfer at a date in the future and a Currency Conversion will be required, there will always be a risk that the currency exchange rate that applies to the transfer when it is processed may be less beneficial to you than if you had instructed us to process the transfer on the same Banking Day.

7. Global Transfers Unsupported Currencies – Instruction times and exchange rates

This clause applies to an Instruction to effect a Global Transfer in a Global Transfers Unsupported Currency.

Cut-off times may apply. These will be the cut-off times applicable to the particular Group member that processes the Instruction for that currency.

If you give an Instruction to us on a Banking Day and request that it be processed immediately, it may not be processed on that same Banking Day if we receive the Instruction at a time after an applicable instruction cut-off time. In that event the Instruction will be processed on the next Banking Day.

If you give an Instruction to make a Global Transfer on a future Banking Day it will be processed on the requested future Banking Day.

In each case, if a Currency Conversion is required, the currency exchange rate that will be applied is the rate that applies at the time the applicable Group member processes the Instruction. The applicable Group member is the Group member with which you hold the account to which the Global Transfer is to be made. That Group member will determine the currency exchange rate.

Please note that due to fluctuations in currency exchange rates, there will always be a risk that the currency exchange rate that applies to a Global Transfer where a Currency Conversion is required may be less beneficial to you than had we been provided with Instructions to effect the Global Transfer on the same Banking Day and prior to the applicable Instruction cut-off time.

8. Agreed limits

You must not make a Global Transfer for an amount which would cause you to exceed any limit agreed with, or imposed by, the Group. There are five (5) types of daily transaction limits applicable to Global Transfers . The maximum daily transaction limits which apply to a 24 Hour Period are:

1. Global limit – USD$100,000 – this is your maximum cumulative limit for all Global Transfers from accounts held with any Group member;
2. Transaction Limit - USD100,000 – this is your maximum limit per single Global Transfer;
3. Group Member Limit – USD100,000 – this is your maximum accumulated limit for transfers made from any one Group member (subject to point 5 below);
4. Customer Limit – Variable per customer to be determined and, if relevant, advised to you by a Group member;
5. Country Specific Limits/rules – some countries in which Group members operate, and where you may have accounts, may have local laws in regards to currency transfers. Please check with the relevant Group member for more details.

When you are not using the Global Transfer service the transaction limits applicable to the Online Banking Service will apply to EFT Transactions.

If you give two Instructions for a Global Transfer with exactly the same details within a short space of time, the second Instruction will be rejected at the point of input.

N.B. Daily transactional limits apply to all fund transfers, including 'Pay Later' and recurring transfers. For example if today you initiate a 'Pay Later' transfer of $20,000 or a recurring transaction of $5,000 over the next 4 weeks, then in both these instances the total funds transfer amount of $20,000 will apply to your transaction limit today. Contact us if you'd like to request an increase to your daily limit.

9. Termination

HSBC reserves the right at any time to, and you may request HSBC at any time to, terminate your access to Global View and / or to remove your access to the function of Global View which permits you to effect Global Transfers.

If your access to the Online Banking Service is terminated for any reason, your access to the function of Global View which permits you to effect Global Transfers will be terminated automatically.

Instructions for Global Transfers which have been given before, but which are scheduled to be made after, your access to the function of Global View which permits you to effect Global Transfers is terminated, may not be processed and HSBC will not be liable should you not make alternate arrangements.

INFORMATION ABOUT GLOBAL TRANSFERS

Significant Benefits

Convenience – You will be able to make a currency transfer from an account you hold with us to an account you hold with another Group member and whether or not the funds in those accounts are held in different currencies.

Significant Risks

Currency Conversion

If your Global Transfer involves a transfer from an account in which funds are held in one currency to an account in which funds are held in a different currency, a Currency Conversion will be required. A Currency Conversion may present the following risks:

- fluctuations in exchange rates may adversely impact on your funds when converting currencies;
- past performance of a currency is not necessarily an indication of its future performance;
- due to fluctuations in currency exchange rates, if a rate of exchange is advised to you on inquiry, it may be different from the rate of exchange that you may obtain subsequently when carrying out the Global Transfer;
- there are time delays in processing transactions during which time the exchange rate may change.

Therefore, you must use your own independent judgment in respect of currency transfers and not rely on any advice, opinions or data supplied by us.

Operational Risk

Operational risk is the risk of loss from disruptions to internal processes, people and systems or disruptions arising from external events. Disruptions resulting from operational risks may affect the processing of your Global Transfer in a timely manner. This may result in an exchange rate applying to the Global Transfer that is less favorable to you.

Termination of Service Risk

In the event that your access to,

the Global Transfers function is terminated you will need to make alternate arrangements for any future dated Instructions for Global Transfers you may have given us.

Costs, Fees and Charges

When you give an Instruction to effect a Global Transfer which requires a Currency Conversion you agree to pay one currency in exchange for another currency. Exchange rates vary depending on a range of factors such as interest rate differentials, economic conditions and government actions.

Although you will not be charged a fee to effect a Global Transfer, other fees or charges may apply for related transactional services. Information about these costs is contained in the booklet, "Personal finances services charges – your guide".

PART C

Supplementary Product Disclosure Statement for HSBC Online Banking

IMPORTANT INFORMATION

This Supplementary Product Disclosure Statement ("**SPDS**") supplements, and is intended to be read with, HSBC Online Banking Product Disclosure Statement (20 March 2013) ("**PDS**") to which it is appended (see Part A).

The date of this SPDS is 1 August 2017.

This SPDS only applies to HSBC Entity Customers who are:

- a Non-Trading Company;
- a Trustee for a SMSF; or
- a Trustee for a Trust

as defined within this SPDS.

This SPDS does not apply to, and need not be read by, a customer who is not a HSBC Entity Customer. For the HSBC Entity Customers, this SPDS provides information on, and includes the Terms and Conditions for the use of the Online Banking Service, which is only applicable to the above defined HSBC Entity Customers.

This SPDS is intended to operate in conjunction with the PDS. However, if there is any inconsistency, this SPDS prevails

Issuer details

This SPDS is issued by HSBC Bank Australia Limited (ABN 48 006 434 162) (AFSL 232 595).

SIGNIFICANT RISKS

Access and Control Risks

In order to access and use the Online Banking Service, you are required to nominate Entity Administrators and Users to access your EFT Accounts on your behalf. Once nominated and set up on the Online Banking Service, Entity Administrators have the ability to establish and set all access entitlements applying to other Entity Administrators and Users. This includes entitlements to view, create and/or authorise payments from your EFT Accounts and the setting of maximum transactional limits applying to each of these persons within limits agreed by you and HSBC. Depending on the entitlements granted to them by an Entity Administrator, a User or Entity Administrator who is authorised to access and make payments from your EFT Accounts, may be able to access and transact on your EFT Account without the involvement or knowledge of any other User or Entity Administrator. It is therefore your responsibility to appoint an appropriate Entity Administrator who is in turn responsible for setting up appropriate persons as Entity Administrators or Users, and to assign appropriate access entitlements to such persons, on your behalf. The risk of this not being done properly is that access to your EFT Accounts may be set up in a manner which is not appropriate for you. You should therefore have

proper controls and processes to address and monitor this.

1. TERMS AND CONDITIONS FOR THE USE OF THE ONLINE BANKING SERVICE BY HSBC ENTITY CUSTOMERS

1.1 Definitions

Where relevant, terms defined in the PDS apply to this SPDS. In addition, the following terms have the following meaning in this SPDS.

"HSBC Entity Customer" includes a Non-Trading Company, a Trustee for a SMSF and a Trustee for a Trust.

"Entity Administrator" means a person you nominate who is empowered to access and use the Online Banking Service, appoint Users, assign transaction limits to apply to Users and assign the nature of each User's access to the Online Banking Service.

"Non-Trading Company" means a company controlled by a retail client and which HSBC in its discretion deems a retail client subject to any applicable legislation.

"SMSF" means a self-managed superannuation fund as defined in the Superannuation Industry (Supervision) Act 1993 (Cth).

"Trustee for a SMSF" means the trustee(s) for a SMSF.

"Trustee for a Trust" means a trustee for a trust that HSBC in its discretion deems a retail customer subject to any applicable legislation.

"User" for the purposes of this SPDS means you and any other person, who including an Entity Administrator is authorised by you and HSBC to use the service to access and operate an account alone.

1.2 About these Terms and Conditions

These Terms and Conditions operate together with the terms in the PDS. If there is an inconsistency between these Terms and Conditions and the terms in the PDS, these Terms and Conditions prevail.

For the avoidance of doubt, the definition of "Terms" in clause 1.1 of the PDS is to be read as including these Terms and Conditions, applying to the use of the Online Banking Service.

1.3 Acceptance

You agree to the Terms and Conditions for the use of the Online Banking Service when, having been presented with these Terms and Conditions on our website (www.hsbc.com.au) as part of the Combined Product Disclosure Statement and Supplementary Product Disclosure Statement, a User clicks the "Accept" button indicating acceptance of the Terms and Conditions.

2. HSBC ENTITY CUSTOMERS

These Terms and Conditions only apply to HSBC Entity Customers who are:

- a Non-Trading Company;
- a Trustee for a SMSF; or
- a Trustee for a Trust.

2.1 Entity Administrators and Users

You must appoint at least one Entity Administrator.

An Entity Administrator:

(a) appoints Users;

(b) assigns the nature of each User's access to the Online Banking Service – i.e. to effect transactions on EFT Accounts and/or view EFT Account information and request transactions to be made); and

(c) assigns transaction limits to apply to Users within limits agreed by you and HSBC.

An Entity Administrator can also use the Online Banking Service to effect transactions and view information. Once set up, an Entity Administrator can appoint Users directly to perform tasks on the Online Banking Service for you.

The Entity Administrator appoints Users on your behalf.

2.2 Access Entitlements

Once appointed by you and in accordance with your account opening documents, an Entity Administrator will have responsibility for the setting up of Users, and to establish and maintain the access entitlements that are to be granted to each Entity Administrator or User who accesses your EFT Accounts via the Online Banking Service.

The Entity Administrators and Users which are appointed to act on your behalf and the maximum transactional limits which apply to such persons for transactions via the Online Banking Service can be different to the authorised signatories appointed by you. If you wish for access to your EFT Accounts to be consistent between the Online Banking Service and signing instructions, it is your sole responsibility to ensure that these are set up and maintained consistently. HSBC has no obligations or responsibilities whatsoever in this regard.

2.3 Agreed Limits

Clause 1.9 titled "Agreed limits" of the PDS is deleted in its entirety and replaced with the following clause:

Users must not use an Access Method to withdraw funds in excess of any limit agreed with HSBC. If an EFT Account goes over the agreed limit, HSBC may permit a User to use the Access Method,

but you must deposit funds to bring the EFT Account within its agreed limit without unreasonable delay. All limits are in Australian Dollars and may change from time to time. Merchants, our agents and other financial institutions may impose their own restrictions on the amount of funds that may be withdrawn, paid or transferred. There are 4 types of daily transaction limits applicable to each User. The maximum daily transaction limits are set out in the table below:

Transfer Types	Default daily entity limits	*Default daily user limits^
Transfers between EFT Accounts (including foreign currency transfers**)	$500,000	$500,000
Transfers between EFT Accounts and third party accounts.	$50,000	$50,000
Transfers between EFT Accounts and pre-designated third party accounts (including foreign currency transfers**). Note: Transfers of this type are only available on request and is subject to our approval. Processing time is required.	This facility is only available on request. Should we make this facility available to you the default limit is $100,000. The maximum limit you may request is up to $250,000	This facility is only available on request. Should we make this facility available to you the default limit is $100,000. The maximum limit you may request is up to $250,000
BPAY®	$25,000	$25,000

* The default daily user limit figures in this table refer to the daily limits that apply to each User. However, the default daily entity limits may affect the default daily user limits. If you have two Users, for example, even though each User is capable of effecting daily transfers "between EFT Accounts" of up to $500,000, to the aggregate amount of the transfers by the Users must not exceed the default daily entity limit of $500,000.

** The maximum foreign currency transfer Instruction limit is $50,000 per Instruction where instantaneous real-time pricing is not available. Where a foreign currency transfer Instruction is provided after the relevant Payment Cut-off Time, HSBC will apply the currency exchange rate that applies at the time of the Instruction in order to calculate the Australian dollar value for the purposes of daily transaction limits. However, when HSBC processes the Instruction HSBC will apply the currency exchange rate that applies at the time of the processing and that exchange rate may be different from the exchange rate that applied at the time the Instruction was provided.

^ Limits apply at an Online Banking Service level and not at an account level. This means that, for example, if you have 4 EFT Accounts which you access via the Online Banking Service and a daily entity limit of $500,000, this will apply as one limit to transactions which you perform across all of the 4 EFT Accounts and is not a limit of $500,000 per account.

N.B. Daily transactional limits apply to all fund transfers, including 'Pay Later' and recurring transfers. For example if today you initiate a 'Pay Later' transfer of $20,000 or a recurring transaction of $5,000 over the next 4 weeks, then in both these instances the total funds transfer amount of $20,000 will apply to your transaction limit today. Contact us if you'd like to request an increase to your daily limit.

2.4 Amendments to Use of Online Banking Service

You should be aware that once information about an Entity Administrator or User is registered within the Online Banking Service, the information is unable to be edited through the Online Banking Service. This includes but is not limited to details such as Entity or User name, address, email, telephone and fax numbers, mailing address, date of birth, annual income, number of dependents, occupation and name of employer. To amend any of these or other details, written authority with "wet signature" is required to be sent to HSBC and processed before these changes can take place.

For the purposes of this SPDS, in clause 2.2 titled "Use of the Online Banking Service" of the PDS, subclauses 2.2(g) and 2.2(i) are deleted.

2.5 Customer Service and Enquiries for HSBC Entity Customers

Please read these Terms and Conditions together with the terms in the PDS before using the Online Banking Service.

If you do not understand any part of them, or if you have any questions, please call HSBC on 1300 131 607 Monday to Friday from 8am to 6pm or +61 29005 8115 if calling from overseas.

Issued by HSBC Bank Australia Limited ABN 48 006 434 162 AFSL No. 232595
HBAA023PDS a (R12) 01/18

HSBC