

Business Internet Banking

Product Disclosure Statement

HSBC Bank Australia Limited ABN 48 006 434 162 AFSL No: 232595 2 March 2010



The world's local bank

Important Information

This Product Disclosure Statement (PDS) is issued by HSBC Bank Australia Limited.

This PDS is made up of this core document and one about fees and charges.

This PDS is dated as of the latest date borne by either of the documents which comprise it. This core document is dated 2 March 2010.

This PDS sets out the terms and conditions which apply to Business Internet Banking ("Internet Banking Service") issued by HSBC Bank Australia Limited (referred to as "**HSBC**", "**we**", "**our**" or "**us**").

This PDS should be read in full before you make a decision to acquire the Internet Banking Service from HSBC.

All information provided in this PDS is general and does not take into account your individual objectives, financial situation or specific needs. We recommend that after reading this PDS you establish whether, given your circumstances, the Business Internet Banking is suitable to you. If you do register for Business Internet Banking, then we strongly recommend you retain this PDS for future reference.

Information in this PDS is subject to change from time to time and may be updated as described in this PDS. If you received this document electronically or if you received any updated information other than in writing, we will provide a paper copy free on request.

Contents

	Page No.
Key Features	1
Significant Risks, Costs and Cooling-off	2
Access To The Internet Banking Service	4
1. General Terms and Conditions	6
1.1 Definitions	7
1.2 Code of Banking Practice	10
1.3 Acceptance	10
1.4 Records and statements	10
1.5 Fees and Charges	10
1.6 Changes to Terms	10
1.7 Business Administrators and Users	11
1.8 Access Entitlements	11
1.9 Agreed limits	12
1.10 Termination	15
1.11 Electronic communications	15
1.12 Contact	16
1.13 Governing law	17
2. Internet Banking Service	17
2.1 About these Terms	17
2.2 Use of the Internet Banking Service	17
2.3 Access to the Internet Banking Service	18
2.4 Processing Instructions	19
2.5 Electronic advertising	19
2.6 Internet Banking Service security	19
2.7 Bill payments - BPAY [®] Scheme	20
3. Security of Access Methods	22
3.1 Protecting Access Methods	22
3.2 Guidelines	22
4. Internet Trade Services	25
4.1 Availability of Internet Trade Services	25
4.2 Internet Trade Services functionality	25
5. Reporting Loss, Theft Or Unauthorised Use Or Breach Of PIN Or Security Code Security Etc	26
6. Liability For Unauthorised Transactions	26
6.1 Authorised transaction	26
6.2 When you are not liable	26
6.3 When you are liable	27
6.4 Electronic system malfunctions	28
7. Procedures For Handling Errors And Investigating And Resolving Complaints	29
7.1 How to lodge a complaint	29
7.2 Customer Relations	29
7.3 HSBC's investigations	29
7.4 Financial Services Ombudsman	30

HSBC Business Internet Banking - Key Features and Benefits

The Internet Banking Service is a service that HSBC makes available through the internet network to enable the electronic receipt and transmission of information and instructions.

It is an alternative way to do your banking, 24 hours a day, 7 days a week. When Users/Business Administrators log-in to the Internet Banking Service, they can, depending on the authority given to them, perform the following:

- ▶ Check the balance of your EFT Accounts
- ▶ Check currency rates
- ▶ Transfer funds to any accounts within HSBC
- ▶ Transfer funds to other accounts in Australia and overseas
- ▶ Set up and manage re-occurring payments
- ▶ Pay bills displaying the B_{PAY}[®] symbol
- ▶ Request a copy of a previous statement
- ▶ Stop or cancel a cheque
- ▶ Request a PIN for use with Phone Banking
- ▶ Change your Password
- ▶ Place an order for the purchase or sale of foreign currency which is to be transferred between your EFT Accounts
- ▶ Request a document, staff contact or interview with an HSBC representative
- ▶ Send secure emails to HSBC via the Internet Banking secured site
- ▶ Access Internet Trade Services (access to these require relevant HSBC trade facilities)
- ▶ Use autoPay to make up to 100 bulk domestic payments with a single debit transaction
- ▶ Give instructions to utilise existing Foreign Exchange Contracts.
- ▶ Access third party (company) accounts (requires approval from third party)

(Note: Depending on the type of account(s) you hold and the specific Services available to you, you may not be able to access all the above features. Service features may be amended and may change from time to time.)

Significant Risks, Costs and Cooling-off

Significant risks

Internet and computer

You are responsible for acquiring and maintaining any equipment required for continued access to and use of the Internet Banking Service (such as a modem or computer). All reasonable steps must be taken to protect the computer hardware and software including ensuring that an appropriate firewall and/or other protective measures such as anti-virus software are installed on the computer and that the computer is free of viruses. If you do not take adequate internet security precautions there is a risk your security may be compromised which could lead to unauthorised and fraudulent transactions.

In accessing the Internet 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.

Access and control risks

In order to access and use the Internet Banking Service, you are required to nominate Business Administrators and Users to access your EFT Accounts on your behalf. Once nominated and set up on the Internet Banking Service, Business Administrators have the ability to establish and set all access entitlements applying to other Business 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. Depending on the entitlements granted to them by a Business Administrator, a User or Business 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 Business Administrator. It is therefore your responsibility to appoint an appropriate Business Administrator who is in turn responsible for setting up appropriate persons as Business 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 your business. You should therefore have proper controls and processes within your business to address and monitor this.

Compromise of access methods

In order to access and use the Internet Banking Service, you will be provided with various Access Methods. This includes secret codes such as your Username, PIN, and Password and, if you have been issued a Security Device for use with the Internet Banking Service, the Security Device and the Security Code. It is your responsibility to ensure that access to these are not compromised. If this occurs, there is a risk that your accounts will be accessed without your consent and unauthorised transactions may result.

Email and online communication

You can send secure emails to HSBC via the Internet Banking Service. 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.

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 Internet 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 Internet 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 Internet Banking Service.

Access To The Internet Banking Service

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

- ▶ **agreed** to receiving notices regarding the Internet Banking Service by Electronic Communication.

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

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

If HSBC has already received an email address from a User/Business Administrator, 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/Business Administrator 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 Internet 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/Business Administrator to retrieve the communication on www.hsbc.com.au and/or by accessing the Internet 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 Internet Banking Service by Electronic Communication and HSBC is provided with a nominated email address, you will not receive paper notices. If a User/Business Administrator does not provide HSBC with a nominated email address, the User/Business Administrator 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 Internet Banking Service.

AND

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

Other Product Disclosure Statements

You should read these terms in conjunction with the terms and conditions incorporated in your product terms and conditions for relevant HSBC trade facilities and/or Product Disclosure Statements applying to your EFT Accounts accessed via the Internet Banking Service.

About These Terms

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

The Internet 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 Internet Banking Service and, where relevant, the facility terms and conditions governing HSBC trade facilities. If there is an inconsistency between these Terms and the terms and conditions applicable to EFT Accounts accessed using the Internet Banking Service or the terms and conditions applying to HSBC trade facilities, 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 Internet 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 HSBC’s Direct Service Centre on 1300 306 543, or contact your relationship manager if you have one.

Customer Service and Enquiries 1300 306 543 Monday to Friday from 8am to 8pm or +612 9005 8421 if calling from overseas.

Lost or Stolen PINs or Security Devices or Suspected Unauthorised Transactions – internet banking only 1300 306 543

General Terms and Conditions

1. General Terms And Conditions

1.1 Definitions

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 and Business Administrators of the Internet 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, a Security Code, a Username, a Password or any combination of these.

“autoPay” means a service provided by HSBC that permits a User/ Business Administrator to use the Internet Banking Service to make up to 100 bulk domestic payments with a single debit transaction from an EFT Account.

“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.

“Business Administrator” means a person you nominate who is empowered to access and use the Internet Banking Service, appoint Users, assign transaction limits to apply to Users and assign the nature of each User’s access to the Internet Banking Service.

“EFT Account” means an account held by you with HSBC and which HSBC authorises you to access and/ or conduct EFT Transactions on via the Internet Banking Service. Where a third party holds an account with HSBC and requests that HSBC allow and authorise you to access and/ or conduct EFT Transactions on their account via your Internet Banking Service, a reference to “EFT Account” includes these accounts held by a third party and which HSBC has agreed for you to access and/ or

conduct EFT Transactions on via your Internet Banking Service.

“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 one or more Users or by a Business Administrator (or a Business Administrator and a User together) through Electronic Equipment using an Access Method.

“Electronic Communication” means a message HSBC transmits to a User or Business Administrator and the User or Business Administrator receives from HSBC electronically, in a form that the User or Business Administrator 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 Internet Banking.

“FEX Contract” means a foreign exchange contract.

“FEX Contract Number” means the foreign exchange contract reference number given to you (or to a User or Business Administrator on your behalf) in respect of a FEX Contract.

“HSBC, we, our or us” means HSBC Bank Australia Limited ABN 48 006 434 162.

“HSBC 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.

“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 Internet Banking Service by use of an Access Method.

“Internet 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).

“Internet Trade Services” means the HSBC trade services described in clause 4 that can be accessed using the Internet Banking Service.

“Password” means the code comprising alpha-numeric characters chosen by a User or Business Administrator to be used with the Username to access the Internet Banking Service.

“Payment Cut-off Time” means the time in Sydney after 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 or Business Administrator and by which HSBC identifies a User or Business Administrator for Internet Banking.

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

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

“Security Device” means the physical device which HSBC may provide to each User or Business Administrator, which generates a

new Security Code at predetermined intervals. The Security Device remains HSBC’s property at all times

“Service” or **“Internet Banking Service”** means the Internet Banking Service

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

“Unauthorised” means without the knowledge or consent of a User or Business Administrator.

“Unauthorised EFT Transaction” means an electronic funds transfer from an EFT Account initiated through Electronic Equipment using an Access Method without the knowledge or consent of a User or Business Administrator.

“User” means you and any other person authorised by you (or by a Business Administrator on your behalf) and HSBC to access and use the Internet Banking Service to access and/or operate an EFT Account.

“Username” means the code comprising alpha-numeric characters set up by a User or Business Administrator to be used with the Password and Security Code to access the Internet 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 a corresponding meaning.

1.2 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.

1.3 Acceptance

These Terms are provided to you before your registration for the Internet Banking Service on our website (www.hsbc.com.au). You agree to these Terms when a User or Business Administrator clicks the "Accept" button indicating acceptance of these Terms on your behalf.

1.4 Records and statements

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 Internet 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 Internet Banking Service.

1.5 Fees and Charges

If the Internet 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 Internet Banking Service are detailed in the relevant fees and charges guide (at the time the relevant transaction is undertaken), available from any HSBC branch. If your business has a relationship manager, please ask your relationship manager for a copy.

1.6 Changes to Terms

HSBC reserves the right to change these Terms and any other information it has issued about the Internet 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.

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 1.6 may be given electronically in accordance with clause 1.11.

1.7 Business Administrators and Users

Unless you were first issued with the HSBC Internet Banking Service prior to 22 April 2007, you must appoint at least one Business Administrator.

A Business Administrator:

- (a) appoints Users;
- (b) assigns the nature of each User's access to the Internet 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.

A Business Administrator can also use the Internet Banking Service to effect transactions and view information. Once set up, a Business Administrator can appoint Users directly to perform tasks on the Internet Banking Service for you. The Business Administrator appoints Users on your behalf.

If you were issued with an HSBC internet banking service prior to 22 April 2007, all "delegates" (under the old HSBC internet banking service), will automatically operate as Users and unless you wish to have more Users appointed, assign new transaction limits or change the nature of a User's access to the Internet Banking Service, you will not be required to appoint a Business Administrator.

The access of a Business Administrator or a User to your EFT Accounts using the Internet Banking Service is governed by the relevant provisions of these Terms. You must ensure that each Business Administrator and 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 Business Administrators and Users. Your cancellation of a User's or Business Administrator's authority will not be effective until your notification of the cancellation is received by HSBC. You should ensure that all Users/Business Administrators are provided with a copy of these Terms.

1.8 Access Entitlements

Once appointed by you, a Business 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 Business Administrator or User who access your EFT Accounts via the Internet Banking Service.

Except where your EFT Accounts are governed by the "Small Business Deposit Account Product Disclosure Statement", your Business Administrator can elect on your behalf to operate your EFT Accounts via Internet Banking on a:

- ▶ dual payment authorisation method (where the involvement

of two people are required in order to effect a payment from an EFT Account); or

- ▶ a sole payment authorisation method (where the involvement of only one person is required in order to effect a payment from an EFT Account).

Where your EFT Accounts are governed by the “Small Business Deposit Account Product Disclosure Statement”, your use of the Internet Banking Services is only available on a sole payment authorisation method basis.

The Business 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 Internet Banking Service can be different to the authorised signatories appointed by you for the signing of instructions on your account mandate. If you wish for access to your EFT Accounts to be consistent between the Internet Banking Services 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.

1.9 Agreed limits

Users and Business Administrators 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 or Business Administrator to use the Access Method, but you must deposit funds to bring the EFT Account within its agreed limit without unreasonable delay.

There are 5 types of daily transaction limits applicable to each User and Business Administrator. All limits are in Australian dollars. Where a transaction involves a foreign currency, 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 these Instructions 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.

The daily transaction limits are:

Transfer types	Business Limits*	Business Administrator/ User Limits*
Transfers between your EFT Accounts	Your daily transaction limit is \$500,000**	The daily limit on transfers by any single Business Administrator or User (provided the business limit is not exceeded) is \$500,000**
Transfers between your EFT Accounts and third party accounts	Your daily transaction limit is \$20,000** (You may request a higher business limit up to \$100,000**.)	The daily limit on transfers by any single Business Administrator or User (provided the business limit is not exceeded) is \$20,000** (You may request that a Business Administrator or User be assigned a lower limit, or a higher limit up to \$100,000** and provided the business limit is not exceeded.)
Transfers between your EFT Accounts and pre-designated third party accounts	Transfers of this type are only available on request. Should we make this facility available to you, we may impose a limit of \$100,000**	Should we make this facility available to you, we may impose a limit of \$100,000** for any single Business Administrator or User (provided the business limit is not exceeded). (You may request that a Business Administrator or User be assigned a lower limit, or a higher limit up to \$100,000** and provided the business limit is not exceeded.)

BPAY®	Your daily transaction limit is \$20,000** (You may request a higher business limit up to \$50,000**.)	The daily limit on transfers by any single Business Administrator or User (provided the business limit is not exceeded) is \$20,000** (You may request that a Business Administrator or User be assigned a lower limit, or a higher limit up to \$50,000** and provided the business limit is not exceeded.)
autoPay	Transfers of this type are only available on request. Should we make this facility available to you, we may impose a limit of \$20,000**	Should we make this facility available to you, we may impose a limit of \$20,000** for any single Business Administrator or User (provided the business limit is not exceeded). (You may request that a Business Administrator or User be assigned a lower limit, or a higher limit up to \$20,000** and provided the business limit is not exceeded.)

* Business Limits apply at an Internet 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 Internet Banking Service, a Business Limit of \$500,000 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.

**This is the default limit. You may set up a lower limit for a Business Administrator or User at your election. Higher daily limits are also available in certain circumstances upon request, subject to our approval. Please consult your relationship manager for more information.

You determine each type of daily transaction limit for each Business Administrator in the internet banking application document(s). A Business Administrator determines the daily transaction limits for each User.

The holder of a third party EFT Account may, if permitted by HSBC, grant your nominee/s access to that EFT Account and authorise your nominee/s to conduct EFT Transactions on the third party's EFT Account. In which case, unless we state otherwise in any applicable forms, the third party EFT Account holder may authorise you

to determine (subject to the daily transaction limits in the table above):

- ▶ the type and amount of daily transaction limits applying to each Business Administrator; and
- ▶ the daily business limit applying to the EFT Account(s).

A nominee who is also a Business Administrator will determine the daily transaction limits for each other nominee (User).

Where a holder of a third party EFT Account and HSBC has granted your nominee/s access to the third party's EFT Account, the third party EFT Account holder will not be able to use the Internet Banking Service to conduct EFT Transactions (unless your nominee/s authorise the third party EFT Account holder to have access to the third party's EFT Accounts). Additionally, the sum of all EFT Transactions effected in respect of your EFT Accounts and all third party EFT Accounts accessible by your nominees will be subject to the daily business limits and User/Business Administrator limits referred to in the table above.

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 Internet Banking Service at any time by giving

written notice to HSBC.

HSBC may terminate the Internet Banking Service at any time by giving you a written notice.

HSBC may suspend or cancel an Access Method or deactivate a Security Device at any time without notice if it believes the Access Method or Security Device is being misused, there is concern as to the security of the Access Method or Security Device or there is non-compliance with the Terms.

When an Access Method has been cancelled by you or HSBC, Users and Business Administrators must not attempt to use the cancelled Access Method again. If de-activated, the Security Device must be returned by you and/or your Users/Business Administrators.

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

1.11 Electronic communications

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

- ▶ sending an email to an email address nominated by you or a User or Business Administrator; or
- ▶ making the information available at our website www.hsbc.com.au or through the Internet Banking Service, for retrieval by a User or Business Administrator (after notifying the User or Business Administrator by email to the email address nominated by the User or Business Administrator that the information is available for retrieval and the nature of the information and providing the User or Business Administrator with the ability to retrieve the information through our website or through the Internet Banking Service).

If you agree to the above, then:

- ▶ if you, or a User or Business Administrator has on your behalf, provided a nominated email address, you will not receive paper copies of the relevant information;
- ▶ the relevant User or Business Administrator will need to regularly check to see if he or she has received emails from us;
- ▶ the relevant User or Business Administrator will need to maintain and check their electronic address regularly to ensure it is always capable of receiving an Electronic Communication; and

- ▶ the relevant User or Business Administrator will be responsible for printing or saving important information – and we strongly recommend that Users or Business Administrator do so.

You may at any time by notice to HSBC terminate your agreement to receive information by Electronic Communication one or more of the methods above. If a User/Business Administrator does not provide HSBC with a nominated email address, the User/Business Administrator 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 Internet Banking Service. If this occurs HSBC will advise you that the Internet Banking Service has been terminated.

1.12 Contact

You can contact HSBC by:

- ▶ telephoning us on 1300 306 543 Monday to Friday from 8am to 8pm or +612 9005 8421 if calling from overseas.; or
- ▶ writing to us at GPO Box 5302, Sydney NSW 2001.
- ▶ telephoning your relationship manager.

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".

1.13 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. Internet Banking Service

2.1 About these Terms

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

2.2 Use of the Internet Banking Service

Depending on the authority given to a User and the type of EFT Account, the Internet 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 statements be issued 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) view non electronic direct standing order payment instructions in relation to any EFT Account, make BPAY[®] payments from any EFT Account,
- (h) make BPAY[®] payments from 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 Internet Banking Service,
- (k) place orders for the purchase or sale of foreign currency. 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,
- (l) subject to clause 4, access Internet Trade Services,
- (m) use autoPay to make up to 100 bulk domestic payments with a single debit transaction,
- (n) access third party (company) accounts,
- (o) utilise foreign exchange (FEX) contract numbers to provide instructions in respect of existing FEX Contracts.

2.3 Access to the Internet Banking Service

You agree that any person who supplies HSBC with:

- (a) if HSBC has issued a User/Business Administrator with a Security Device, the User's/Business Administrator's PBN, PIN and Security Code; or
- (b) if HSBC has never issued a Security Device to a User/Business Administrator, the User's/Business Administrator'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:

- (c) if HSBC has issued a User/Business Administrator with a Security Device, the User's or Business Administrator's Security Code and the Username and Password; or
- (d) if HSBC has never issued a Security Device to a User or Business Administrator, the User's or Business Administrator's Username and Password,

that person may be allowed access to the Internet Banking Service and to any EFT Account. Once a User/Business Administrator has accessed the Internet Banking Service, HSBC may ask the User/

Business Administrator to enter the Security Code (if the User/Business Administrator has been issued with a Security Device) 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.

HSBC may specify limits on transaction types and values in respect of certain EFT Accounts or the use of the Internet Banking Service and may refuse to act on an Instruction if a transaction exceeds a particular limit. 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 and a Business Administrator's PBN or PIN at any time, by notifying the User/Business Administrator in writing. Users/Business Administrators may change their PIN for use with Phone Banking, or Password at any time.

2.4 Processing Instructions

If a User/Business Administrator gives an Instruction to make a transfer from an EFT Account before the Payment Cut-off Time on a Banking Day, such transfer will be processed on that day.

If a User/Business Administrator gives an Instruction to make a transfer from an EFT Account on a day which is not a Banking Day, or after the Payment Cut-off Time on a Banking Day, such transfer will be processed on the next Banking Day.

A BPAY[®] Payment may take longer to be credited to a Biller if a User/Business Administrator 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 HSBC Group on the website through which the Internet 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 Internet Banking Service.

2.6 Internet 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 your responsibility to ensure that your and your User's/Business Administrator's ability to use the Internet Banking Service is permitted by local law and HSBC shall not be liable for any loss or damage suffered by you or a User/Business Administrator as a result of not being able to use the Internet Banking Service in these jurisdictions.

You and your Users/Business Administrators are responsible for acquiring and maintaining any equipment required for continued access to and use of the Internet Banking Service (such as a computer), and for your computer's anti-virus and security measures. You must, and you must ensure that your Users and Business Administrator must, take all reasonable steps to protect the security of any computer hardware and software and all Access Method, including by ensuring:

- (a) a computer is free of viruses;
- (b) a computer is not left unattended while they are logged on to the Internet Banking Service;
- (c) a computer is free of any form of program or mechanism capable

of recording the PIN, Username or Password; and

- (d) that all windows of the browser used to access the Internet Banking Service are shut down and that the “back” function or similar function cannot be used to trace your activities.

You and your Users/Business Administrators agree not to interfere with or damage (or attempt to interfere with or damage) any PBN, PIN, Username, Password, Security Code, Security Device, data or software associated with the Internet Banking Service.

2.7 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 Internet Banking Service. These provisions operate in conjunction with these Terms as well as the terms and conditions applicable to EFT Accounts accessed using the Internet 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.

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

(a) BPAY® payment instructions

- (i) the Username and Password;
- (ii) where requested by HSBC, the Security Code (where a Security Device has been issued to the User/Business Administrator);
- (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 (eg. 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/Business Administrator's responsibility to allow for sufficient time for processing of payments to the Biller.

Users/Business Administrators 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 order 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/Business Administrator 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 B_{PAY}[®] Payment, allowing HSBC to obtain from that Biller information about your account with that Biller or the B_{PAY}[®] Payment, including your customer reference number and such information as is reasonably required to investigate the B_{PAY}[®] 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 B_{PAY}[®] Payment.

(d) Consequential damage and indemnity

Subject to the Terms:

- (a) HSBC is not liable for any consequential loss or damage you may suffer as a result of using the B_{PAY}[®] 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 B_{PAY}[®] Scheme and will do so without notice if HSBC suspects a User/Business Administrator, or someone acting on your behalf, of being fraudulent.

B_{PAY}[®] Payments for which Instructions have been given and which are scheduled to be made while your right to participate in the B_{PAY}[®] Scheme is suspended will not be processed by HSBC.

3. Security of Access Methods

3.1 Protecting Access Methods

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

3.2 Guidelines

These guidelines should be followed by Users/Business Administrators to ensure the security of an Access Method.

3.2.1 To protect the Identifier:

- ▶ Do not tell or give the Identifier to anyone.
- ▶ Take care to prevent anyone seeing the Identifier when entering it at Electronic Equipment.

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 Security Device.
- (f) Do not record a PIN or Password on anything which is kept with or near a Security Device 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 Security Device, 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) Users should not select a PIN or Password which represents their birth date as a numeric code, or an alphabetical code which is a recognisable part of their name, their telephone number or anything else that could be associated with them.
- (j) 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 Security Device whenever possible.
- (b) Always keep the Security Device 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 Security Device.
- (d) Do not record a PIN or Password or an Identifier on anything which is kept with or near a Security Device without making a reasonable attempt to disguise the PIN or Password or Identifier.
- (e) Do not lend the Security Device 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 Security Device behind after making an EFT Transaction.
- (h) Do not drop the Security Device or expose it to high heat, liquids or attempt to disassemble the Security Device.
- (d) view import bill instructions and submit bill acceptance and bill payment instructions; and
- (e) view export documentary credit transfers and submit transfer documentary credit instructions.

Since the Internet Trade Services is a channel to provide instructions to utilise your existing trade facilities with HSBC, the daily transaction limits in clause 1.9 will not apply to Internet Trade Services.

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

The use of Internet Trade Services by a User/Business Administrator is subject to the facility terms and conditions applying to HSBC trade facilities (as amended from time to time).

4. Internet Trade Services

4.1 Availability of Internet Trade Services

Internet Trade Services are only available if you have been provided with relevant and necessary HSBC trade facilities required to access Internet Trade Services.

You authorise us (and any relevant member of the HSBC Group) to act on Instructions provided by Users/ Business Administrators through the Internet Banking Service in respect of (a) – (e) above – whether the Instructions are provided in respect of trade services provided to you, or trade services provided to a third party (subject to the third party consenting to you and Users/ Business Administrators providing us with Instructions through the Internet Banking Service).

4.2 Internet Trade Services functionality

A User/Business Administrator can use Internet Trade Services to:

- (a) view information regarding import and export accounts, trade facilities and trade authorisations;
- (b) submit import documentary credit applications and requests;
- (c) create and amend frequently used templates and trade services clauses;

An Instruction provided to HSBC through the Internet Banking Service is taken to be an instruction given under the relevant facility terms and conditions governing your HSBC trade facilities.

Use of Internet Trade Services may be subject to a fee. Please refer to the relevant fees and charges guide for details.

5. Reporting Loss, Theft Or Unauthorised Use Or Breach Of PIN Or Security Code Security Etc

Users/Business Administrators must notify HSBC immediately if a PIN or Password becomes known to someone else, if a Security Device is misused lost or stolen or if a transaction is suspected to have been made on an EFT Account without a User's/Business Administrator's authority. Users/Business Administrators 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/Business Administrator has been fraudulently induced to make a BPAY[®] Payment. Users/Business Administrators should notify HSBC in Australia by calling us on 1300 306 543. If overseas, Users/Business Administrators should report to any branch of an HSBC Group member bank or call +612 9005 8187.

HSBC will acknowledge the notification by giving the User/Business Administrator 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. HSBC will then cancel the Access Method (involving, if relevant, deactivating the Security Device), and arrange for the User/Business Administrator to select a new one, as appropriate.

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.

6. Liability For Unauthorised Transactions

6.1 Authorised transaction

Subject to clauses 6.2 and 6.3 below, you are liable for all EFT Transactions carried out in respect of your EFT Accounts.

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/Business Administrator

has received the PIN or Security Device which forms part of their Access Method;

- (b) after HSBC receives notification that a PIN, Username, 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 you and/or your User/Business Administrator have not contributed to the loss; or
 - (f) caused by the same transaction being incorrectly debited more than once to the same EFT Account.
- (c) voluntarily disclosing the PIN, or Password to anyone, including a family member or friend;
 - (d) (where the User/Business Administrator has been issued with a Security Device) voluntarily disclosing the PIN, or Password and showing the Security Device or otherwise disclosing the Security Code to anyone, including a family member or friend;
 - (e) (where the User/Business Administrator has been issued with a Security Device) voluntarily disclosing the PIN, or Password or showing the Security Device (or otherwise disclosing the Security Code), but not all (PIN/ Password and Security Device), 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;

6.3 When you are liable

Where HSBC proves on the balance of probabilities that you and/or your User/Business Administrator have contributed to the losses in respect of an EFT Account resulting from an Unauthorised EFT Transaction by:

- (a) the User's/Business Administrator's fraud;
- (b) (where the User/Business Administrator has not been issued with a Security Device)

- (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 Security Device (without making any reasonable attempt to protect the security of the record of the PIN, Username, Password or Security Device) 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 Security Device (without making any reasonable attempt to protect the security of the record of the PIN and PBN or Username, Password or Security Device), 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;

- (i) or 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 Security Device, Unauthorised use or breach of PIN, Username, Password or Security Code security.

Where HSBC proves on the balance of probabilities that the User/Business Administrator 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 Security Device 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/Business Administrator 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.

6.4 Electronic system malfunctions

We will make all reasonable efforts to ensure that the Electronic Equipment or system provided by or on behalf of us is operational and is functioning correctly. We are not liable to you if

that Electronic Equipment or system does not accept a User's/Business Administrator's Instructions, or if an Access Method fails to operate the Electronic Equipment or system.

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/Business Administrator's Instructions but failing to complete the transaction. However, if the User/Business Administrator 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/Business Administrators should make a note of the time of the malfunction and the amount involved and report the malfunction to HSBC.

You are at all times responsible for your own Electronic Equipment.

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 if you 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 have a complaint or concern if relevant, 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. If you have a relationship manager, any complaint or concern should be made known to them.

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 11, 580 George Street Sydney NSW 2000

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

Our front line staff, managers or Customer Relationship team should be able to resolve any issues you raise. 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.

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

- ▶ the result;
- ▶ the reasons for its decision with reference to the relevant provisions of the Terms; and
- ▶ 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 Services Ombudsman.

7.4 Financial Services Ombudsman

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

The FOS cannot investigate:

- ▶ a claim for more than \$500,000;

- ▶ a claim in relation to a commercial decision by HSBC, such as whether a loan is approved; or
- ▶ 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 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

BPAY® is a registered trademark BPAY Pty Ltd ABN 69 079 137 518.

Issued by HSBC Bank Australia Limited ABN 48 006 434 162 AFSL 232595