EFTsure Privacy and Confidentiality Statement

1 About this Privacy Statement and Confidentiality Commitment

This Privacy Statement and Confidentiality Commitment is made by EFTsure Pty Limited ABN 21 168 403 736 (**EFTsure**), an Australian owned and operated business that provides electronic payment verification services to Australian businesses.

This Privacy Statement and Confidentiality Commitment:

- sets out how we collect, use and disclose personal information entrusted to us by our customers or otherwise collected and used by us;

- states our commitments to each customer that entrusts us with recipient names and account numbers for verification. Our key commitments are:

  (1) that EFTsure will maintain business confidentiality and will not disclose that a particular customer deals with particular persons and entities except for the purpose of conducting verification of payee details for that customer or otherwise at the request, or with express consent, of that customer,

  (2) that payee names and account details are only to be used or disclosed for the purposes and in the ways described in the EFTsure Privacy Statement and Confidentiality Commitment;

- sets out how we collect, use and disclose other personal information that we collect or that is entrusted to us.

We comply with this Privacy Statement and Confidentiality Commitment and also, in relation to 'personal information' about individuals as regulated by Privacy Laws, comply with Privacy Laws. **Privacy Laws** are the Privacy Act 1988 (C'th) including the Australian Privacy Principles (**APPs**) and all other Australian privacy and data protection laws, mandatory codes and other mandatory requirements.

However, most of the information that we collect, and many of the records that we use and disclose, is not personal information about individuals. We know that each customer that entrusts us with recipient names and account numbers for verification expects us not to disclose that the customer deals with particular persons or entities except for the purpose of conducting verification of payee details for that customer or otherwise at the request, or with express consent, of that customer. We accordingly undertake to customers and prospective customers that we will not and do not disclose to other persons or entities the identity of particular persons and entities with whom each of our customers deal, instead retaining, using and disclosing records of the identity of businesses with verified details and of failed verifications only for the purposes and in the ways described in this Privacy Statement and Confidentiality Commitment.

We will not modify key commitments that that EFTsure will maintain business confidentiality and accordingly will not disclose that a particular customer deals with particular persons or particular entities, except for the purpose of conducting verification of payee details for that customer or otherwise at the request, or with express consent, of that customer.

We may modify or amend other provisions of this Privacy Statement and Confidentiality Commitment from time to time. We will display a notice on our website indicating when any such revisions have been made.

This Privacy Statement and Confidentiality Commitment was last updated on 02 May 2018.

The EFTsure service (the **Service**) means the EFTsure payee validation service as described on our Website (as may be changed or updated from time to time by EFTsure via the Website). If you are a

customer or prospective customer for the EFTsure Service you should also read the EFTsure Terms. The EFTsure Terms tell you who EFTsure is and, what we do, and set out other (non-privacy and confidentiality related) terms on which we will provide the EFTsure Service to customers.

2 Why do payers use the EFTsure Service?

The EFTsure Service supports some of Australia's leading businesses by ensuring that payments by them go to the right bank account of intended recipients.

We do this by:

- verifying proposed recipient names, email and other contact and account details and account numbers (as provided to us by our customers for checking) as recorded by our respective customers as prospective payers. We do this by a variety of means, including enquiry made by us of prospective recipients, cross-verification using records of previous verifications that we have conducted in relation to the proposed recipient, and cross-verification by matching multiple requests made by multiple customers; and

- confirming the verification of payee details to our customers as payers before they make payments to the recipient.

Australian inter-bank payment systems do not enable automated checking of payee names against the payee name associated with a bank account. Accordingly, funds may be inadvertently or through fraud deposited into an account that is unrelated to the nominated recipient. This is because Australian inter-bank payment systems treat the payee name as an information field for recording on account statements, but not a required field for verification or verification of payee name against the name recorded in the recipient bank's system as the holder of the bank account specified in the payment record. Payments made to an account number may therefore be credited to that account number without any verification or verification by the bank of the payee name against the name of the account holder.

Our service enables a prospective payee to verify and confirm that their payment details as proposed to be used by a payer are in fact correct, or cross-verification to substantially reduce and mitigate possibilities for fraud by individuals either acting alone or in concert.

Our service provides assurance to:

- our customers, being payers proposing to make direct payments to bank accounts of Australian recipients, that the payment should be received and credited by the recipient bank to the correct recipient and that this recipient holds a bank account with the details as verified by us; and

- prospective payment recipients, that the business making a payment to that recipient has the correct recipient name and that this recipient name is associated with the correct account details.

Our service therefore:

- reduces risk of adverse consequences that otherwise are likely to arise from operator error or inconsistencies in transcription of payee details from invoices or other source material into payee details as held in accounts payable systems;

- reduces opportunities for fraud that otherwise may arise through bank account details being deliberately associated with payee names that are not the holders of those bank accounts;

- improves relationships between our customers and their suppliers and other prospective payees, by ensuring that verification happens once and then through a courteous, confidential and trustworthy procedure that includes a proper audit trail;

- improves banking relationships, by reducing possibilities of misdirected or incorrectly credited payments;

- reduces credit risk. Most banks do not accept contractual responsibility to reimburse their customers for unrecoverable payments that had been credited to an destination account number as notified by their customer where the destination account number is not the intended payee, regardless of whether the intended payee details as entered in the information field of the payment request matched the name of the holder of the destination account number.

3 Why does EFTsure publish this Privacy Statement and Confidentiality Commitment?

In short, our business helps customers ensure that money that they are paying out through the Australian inter-bank payment system gets to the correct recipient.

That is the reason why:

- we collect proposed recipient names, email and other contact and account details and account numbers from our customers for checking,

- we contact prospective payees to check the match of their name and bank account details or conduct cross-verification using records of previous verifications that we have conducted in relation to the proposed recipient or by matching multiple requests made by multiple customers,

- we retain a record of payee details that are verified, and a record of details that we appear incorrect or unverifiable, for disclosure to our customer and also to any future customer making an enquiry as to the same prospective payee, and

- we disclose to our customer and any future customer whether the details that they provided to us about a prospective payee have been verified or not.

Some of our customers make payments to the same payees: for example, the Australian Taxation Office, Australian Post, airlines, electricity and telecommunications service providers, office supply companies and courier companies and so on.

We seek to avoid multiple contacts of the same prospective payee confirming the same details. Upon receiving a request from a customer for verification of a prospective payee and bank account, we may conduct cross-verification using records of payee details as formerly verified by us or by matching multiple requests made by multiple customers and then disclose to our customer whether the details that they provided to us for verification match a previously verified record or not. If there is a cross-verification match in relation to a prospective payee, we may elect not make a further verification enquiry of the prospective payee and we may then verify to our customer that the details that they provided to us appear to be correct. If there is not a cross-verification match, we will undertake the verification process described above.

Our verification process depends upon confirmation by a prospective payee of their bank account details or cross-verification as above described. If a prospective payee does not elect to confirm their bank account provide details, or cross-verification as above described is not possible, we cannot complete our verification process.

We retain, use and disclose records of the identity of businesses with verified account details and of failed verifications only:

- for the purposes described above.

- for otherwise reasonably related secondary purposes such as data analytics and other statistical analysis as to verifications, maintaining an audit trail as to verifications undertaken and the

outcome of those verification enquiries, maintaining business records as required by laws, assisting our customers or banks or law enforcement agencies with investigation of any suspected fraud or other serious wrongdoing, as required by law or otherwise as required or authorised by law, including Privacy Laws.

Except as above described we will not otherwise disclose records of the identity of businesses with verified account details and of failed verifications to any third party unless:

(a) that third party is a group company of ours, in which case we will require that group company to only use and disclose such records in accordance with this Privacy Statement and Confidentiality Commitment as if a reference in this Privacy Statement and Confidentiality Commitment to us was a reference to that group company;

(b) that third party is a sub-contractor engaged to provide services to us. This may include disclosure to contractors outside of Australia and located in countries whose Privacy Laws do not provide a similar or equivalent level or scope of protection of personal information as Australian Privacy Laws. In this case we will obtain contractual commitments by these sub-contractors to only use and disclose such records for the purposes of providing services to us in accordance with this Privacy Statement and Confidentiality Commitment.

We will not use any personal information about an individual for a secondary purpose unless:

(a) for the purposes described above;

(b) an individual would reasonably expect that we would use or disclose the personal information for that secondary purpose and that purpose is related to the primary purposes for which it was given to us;

(c) that individual has consented to the use of that personal information for the secondary purpose; or

(d) the secondary use or purpose is required or permitted under law, such as in connection with the sale of some or all of our business or assets, or the disclosure is authorised by the Privacy Laws including to lessen or prevent a serious threat to life or health, to protect the personal safety of the public, if authorised or required by law, if we have reason to suspect that unlawful activity has been, is being or may be engaged in, to enforce the law or where necessary to investigate a suspected unlawful activity, or if we have told an individual that personal information about that individual is usually used or disclosed to third parties in this way.

4 What is personal information?

Personal information is information or an opinion about an individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in material form or not.

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

Personal information may be either collected directly by us or provided (disclosed) to us by someone else.

There is a type of personal information called 'sensitive information' that is subject to more stringent obligations. Sensitive information includes information about an individual's health (including predictive genetic information), racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, criminal record, biometric information that is to be used for certain purposes and biometric templates. We do not knowingly collect, hold or use sensitive information.

5 Collection and use of personal information by us

(a) The EFTsure service is provided to assure payers that their payments will go to the correct recipient and prospective payees that payments due to them will be properly credited to their nominated account. EFTsure considers that this is a use of payee information reasonably within the contemplation of prospective payees. As service provider to our customers, we rely upon each customer that entrusts us with proposed recipient names and account numbers and other data, including personal information, to provide any notices and obtain any consents as may be required or desirable to enable the customer to disclose that data, including personal information, to us, so that we may provide the EFTsure service in accordance with this Privacy Statement and Confidentiality Commitment and with Privacy Laws.

(b) APP 3.6 provides that an APP entity must collect personal information about an individual only from that particular relevant individual, unless it is unreasonable or impracticable for the entity to collect personal information only from the individual. Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned depend on the circumstances of the particular case, including whether the individual would reasonably expect personal information about them to be collected directly from them or from another source, the sensitivity of the personal information being collected, any privacy risk if the information is collected from another source and the time and cost involved of collecting directly from the individual. It is not reasonable or practicable for EFTsure to verify that each individual in relation to whom personal information (not being sensitive information) is provided to us by a customer is aware that personal information will be provided by that business to EFTsure.

(c) If you wish to verify how, when and why any business with whom you interact or otherwise deal collects personal information about you or then uses or discloses that personal information to anyone else, you should first check the privacy statement of that business (usually available at their website and labelled privacy policy, privacy statement or something similar) and any privacy notice or other terms associated with a particular product or service that you may consider acquiring or acquire from that business.

6 Direct marketing

We will comply with APP 7 and the *Spam Act* 2003 (Cth) in relation to any direct promotional marketing of our services by us, including:

(a) allowing an individual to opt out of receiving any further direct promotional marketing from us; and

(b) in each written communication from us, setting out our business address, telephone number and, if the communication with that individual is made by fax, telex or other electronic means, a number or address at which we can be directly contacted electronically.

Where we use personal information for the purposes of business to business direct promotional marketing, we rely on the exception in the Privacy Act to do so.

7 Cookies

(a) A cookie is a small file containing information specific to a user, passed through an internet protocol such as a web browser and stored on a device.

(b) We use cookies and other technology to track access to, and use of, our website. The information gathered is not personally identifiable and is used to improve our website.

(c) We may also be provided with cookies data, anonymous identifier data, device information, log information and other information, if provided by ad serving services or advertising networks and

relating to use by other persons of third party websites serviced by those ad serving services or advertising networks. Many browsers and internet access devices are set by default to accept cookies. However, if you do not wish to receive any cookies you may set your browser or configure your internet access device to either prompt you whether you wish to accept cookies on a particular site, or by default reject cookies. Please note that rejecting cookies may mean that some or all of the features and functionality of particular websites or internet services will not be available to you.

8 Quality, access and correction of personal information

(a) Where we collect personal information from an individual directly, we take steps to ensure that the personal information we collect, use and disclose is accurate, up to date and complete. These steps include maintaining and updating any personal information when we are advised by an individual that their information has changed.

(b) Where we collect personal information about an individual from a third party, we rely on that third party to ensure that information it collects is accurate, up to date and complete, subject however to the verification procedures which are at the core of the EFTsure service as above described.

(c) An individual may request access to personal information about that individual that is held by us. Subject to any permitted exception under the Privacy Laws, we shall give that individual access to that personal information.

(d) If an individual notifies us that the information we hold about them is not accurate, we will take reasonable steps to correct that information. To the extent that we have received any personal information indirectly (for example, from a business for which we act as sub-contractor), we may notify that business that it has received a request from an individual to access or correct the personal information it has provided to us.

(e) If you require access to your personal information, please contact www.EFTsure.com.au/contact-us.html. Before we provide you with access to your personal information we will require some proof of identity.

(f) For most requests, your information will be provided free of charge, however, we may charge a reasonable fee if your request requires a substantial effort on our part.

(g) If we refuse to provide you with access to the information, we will provide you with reasons for the refusal and inform you of any exceptions relied upon under the APPs (unless it would be unreasonable to do so).

(h) We take reasonable steps to ensure that your personal information is accurate, complete, and up-to-date whenever we collect or use it. If the personal information we hold about you is inaccurate, incomplete, irrelevant or out-of-date, please contact us and we will take reasonable steps to either correct this information, or if necessary, discuss alternative action with you.

9 Retention of personal information

We retain personal information after we have used the personal information for the purposes for which we collected or received it.

If we retain such personal information, it will only be used for the following purposes:

(a) as required by or under Australian law, or a court / tribunal order;

(b) as required for professional indemnity insurance; and

(c) in accordance with our back-up archive policy.

When no longer required, EFTsure uses its best endeavours to ensure that all such information will be destroyed in a secure manner and in a reasonable time frame.

10 How we hold and secure your personal information

The security of your personal information is important to us.

We take appropriate industry recognised steps to prevent the personal information we hold about you from misuse, interference or loss, and from unauthorised access, modification or disclosure. This includes the use of technologies and processes such as access control procedures, network firewalls, encryption and physical security to protect the privacy of your personal information.

11 Links to other websites

Sometimes our website contains links to other websites. When you access a website other than our website, we are not responsible for the privacy practices of that site. We recommend that you review the privacy policies of each website you visit.

12 How to contact us

(a) If an individual:

(i) would like to access or inquire about any personal information we hold about that individual;

(ii) has a query in relation to this Privacy Statement; or

(iii) would like to make a complaint about out handling of an individual's personal information,

please contact us using the details below.

A: Level 6, 122 Walker Street

North Sydney NSW 2060

E: support@eftsure.com.au

T: 1300 985 976

(b) If you wish to make a complaint about an alleged breach of the Privacy Laws, we ask that you send us your complaint in writing to the email address listed above. We endeavour to respond to complaints within a reasonable period (usually 30 days). If you are not satisfied with our response, you may make a complaint to the Office of the Australian Information Commissioner by phoning 1300 363 992 or by email at enquiries@oaic.gov.au.