

DVS DATA USE AND DISCLOSURE STATEMENT

Transcash International Pty. Ltd. (ACN 147705324) trading as iPay, iSend, and iSend Global (the “Company”, “Transcash”, “we”, “us”, “our”) is a global cross-border payment operator, duly licensed under an Australian Financial Services License issued by the Australian Securities and Investments Commission (ASIC), and registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC).

As an operator of a global cross-border settlement network spanning over 100 countries, we are subject to the provisions of the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs) and remain fully committed to complying with all applicable privacy obligations thereunder. Transcash also affirms its unwavering commitment to the prevention of money laundering, the financing of terrorism, and all other forms of financial crime in accordance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 [“AML CTF Act”] and other relevant legislation.

To this end, we have implemented and maintain robust internal policies and procedures, including our *Anti-Money Laundering and Countering the Financing of Terrorism Policy* and *Data and Privacy Protection Policy*, aimed at detecting, deterring, and reporting unlawful activity and ensuring the secure handling of all personal and sensitive data collected or obtained during our operations.

As part of our obligations under the AML CTF Act, we are required to verify the identification of our customers prior to offering our remittance services. Under our customer identification and verification procedures, we utilize both government and private data sources, including the *Document Verification Service* (“DVS”), a secure online system established under the *Identity Verification Services Act 2023 (Cth)* [“IVS Act”] and governed by the *Identity Verification Rules 2024* [“IVS Rules”]. The DVS allows us to verify the authenticity of identity information provided by our customers against official records.

As an authorized DVS Business User, we are obligated to comply fully with the requirements set forth in the *Document Verification Service Access Policy* [“Access Policy”].

This DVS Data Use and Disclosure Statement (“DVS Statement”) is established to inform our customers (“Customer”, “you”, “your”) of the use of the DVS for identity verification purposes. It ensures that all activities relating to the use of the DVS are carried out in strict

DVS Data Use and Disclosure Statement
Transcash International Pty. Ltd.

compliance with applicable legal, regulatory, and policy requirements, and with the express consent of the Customer, as mandated by relevant laws.

1. Access to the DVS

We shall access the DVS through an approved Gateway Service Provider under a valid service agreement ["Participation Agreement"], entered into with that provider to verify identity documents. Any changes in the Gateway Service Provider shall be subject to a renewed or amended agreement to ensure continuous lawful access.

2. Permitted Use of the DVS

We shall use the DVS strictly for lawful and approved purposes as outlined below:

2.1. Consent from Customers

- a. We shall obtain express, informed, and voluntary consent from individuals prior to initiating DVS matching.
- b. Customers are requested to refer to our Data and Privacy Protection Policy to understand how we collect, handle, and store personal information.

2.2. Authorized Access and Use

- a. Only authorized personnel within the Company may access or request the DVS using the assigned Business User ID.
- b. All Transcash personnel, including Overseas Personnel, shall be appropriately informed of, and shall strictly comply with, the terms of the Participation Agreement and the Access Policy at all times.
- c. Access and use are limited to internal operational purposes for verifying the identity of individuals who have provided express and informed consent.
- d. The DVS shall not be used for marketing, profiling, or sharing data with third parties, unless permitted by law.
- e. We use the DVS solely to facilitate identity verification via authorized government channels, including through Gateway Service Providers. The verification results are based on data provided by official record holders, and we do not independently verify the accuracy or completeness of such data. More information about the verification assistance service is set out in the Attorney-General's Department's Identity Verification Services [Privacy Statement](#).

DVS Data Use and Disclosure Statement
Transcash International Pty. Ltd.

- f. To the extent permitted by law, we do not warrant or guarantee the accuracy, completeness, or reliability of any identity verification outcome obtained through the DVS.
- g. Nothing in this DVS Statement excludes, restricts, or modifies any consumer guarantee, right, or remedy conferred by the Australian Consumer Law (ACL) or other applicable legislation that cannot be lawfully excluded. If you are a consumer under the ACL and we fail to comply with a consumer guarantee in relation to our identity verification services, our liability is limited, to the extent permitted by section 64A of the ACL, to:
 - i. the resupply of the service; or
 - ii. the payment of the cost of resupplying the service, unless it would not be fair or reasonable for us to limit liability in this way.

2.3. Overseas Access

- a. We shall provide prior written notice to the Framework Administrator (the “Authority”, as identified by the Access Policy) of any proposed use of, or access to, the DVS by any entity or individual located outside of Australia or New Zealand who is acting as our employee, agent, contractor, consultant, sub-contractor (at every level) or sub-consultant (at every level) [“Overseas Personnel”];
- b. We shall not allow any entity or individual located outside of Australia or New Zealand to use or access the DVS other than the Overseas Personnel notified to the Authority.
- c. Identity verification may be carried out through verification services located within Australia and overseas, as applicable. Use of such services will comply with all relevant legal and contractual obligations, including any requirements for notice to and approval from the Authority.

2.4. System Integrity and Conduct

- a. We shall not modify, disrupt, interfere with, or misuse the DVS or its functionality in any way, or interfere with or disrupt use of the DVS or allow any such conduct.
- b. The DVS shall not be used for any purpose beyond those authorized under the Participation Agreement and applicable laws.
- c. All DVS Information Match Results shall be logged, recorded, and made available for audit or inspection upon request by the Framework Administrator

or other competent authorities.

3. Security and Confidentiality

- 3.1. We shall comply with all security procedures advised to us in relation to the DVS and take all reasonable action to protect and maintain the security of the DVS and our access to and use of it.
- 3.2. We shall implement robust access controls, monitoring systems, and data protection measures to safeguard personal information from unauthorized access, use, interference, loss, or misuse.
- 3.3. DVS-related information shall not be disclosed except where required or permitted by law.
- 3.4. Any unauthorized access, suspected breaches, or security incidents shall be reported to the Authority without delay.
- 3.5. Individuals affected by such a breach shall be promptly notified where required.

4. Compliance Monitoring and Reporting

- 4.1. We shall comply with all applicable laws, as well as all requirements, instructions, and guidance from the relevant Authority in respect to our access and use of the DVS and Information Match Data.
- 4.2. We shall fully cooperate with and support any audit or verification process initiated by the relevant Authority.
- 4.3. We shall undertake an annual audit of our use of the DVS and our compliance with the provisions of the Participation Agreement, the IVS Rules, and the Access Policy.
- 4.4. A Compliance Statement in the prescribed format shall be submitted annually by the specified due date. It must be signed off by a senior representative and shall include, at a minimum:
 - i. Our use of the DVS during the reporting period and the compliance with the Participation Agreement, IVS Rules, and Access Policy.
 - ii. Disclosure of breaches (if any), including the nature of the breach, date(s), persons involved (if applicable), and remedial action taken.
 - iii. Any recommendations received regarding our use of the DVS.
- 4.5. We shall maintain records and evidence that support the statements made in each Compliance Statement, which shall be made available to the Framework Administrator upon request.

5. Review and Amendments

This DVS Statement shall be reviewed annually and may be updated to reflect any changes in legislation, policy requirements, or operational practices. All updates shall be approved by senior management and communicated to all relevant personnel.

If individuals have any specific needs or require this notice in an alternative format, or if you need assistance due to any special circumstances, please contact us.

6. Consent Statement for Identity Verification via DVS

By proceeding, you acknowledge that you have read and understood this DVS Statement and the following, and you expressly provide your informed and voluntary consent for the use of your personal information for identity verification purposes through DVS:

- a. You confirm that the information you provide is accurate, current, complete, and valid, and that you are authorized to provide the personal details for verification through DVS.
- b. The purpose of DVS use is solely for identity verification, which may be conducted through authorized Overseas Personnel or through verification services located within Australia and overseas, as applicable.
- c. Your personal data will not be used for any unrelated or secondary purposes.
- d. You have the right to refuse consent; however, we may be unable to provide services without completing identity verification.
- e. Your consent must be specific, current, and given by a person with legal capacity to do so.
- f. If you have any concerns regarding the use of your identification information, you may contact Transcash at info@isend.com.sg or via WhatsApp at +61 476 058 772 (WhatsApp). For more information about our complaint handling process, please refer to our Terms and Conditions.
- g. If your concerns remain unresolved, you may escalate the matter to the Attorney-General's Department of Australia, the designated DVS Hub Manager.
 - ☐ By registering for, accessing, or using our Services, you are deemed to have read, understood, and agreed to the terms and conditions set out in this DVS Statement, unless you explicitly opt out in accordance with the provisions of this Statement.