Last Updated: 6/5/2026

Privacy Policy

ABN: 37 640 080 119

William Yau
GREAT INTERNATIONAL PTY LTD T/A GREAT FOREX

1. Introduction

This Privacy Policy is made on behalf of Great International Pty Ltd (ABN 37 640 080 119) trading as Great Forex ("we", "us", or "our"). Any reference to "Great Forex," "we," or "our" in this Privacy Policy refers to Great International Pty Ltd. Great Forex is an Australian-based remittance service company registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC) (Registration Number: IND 100663273-001)

We are committed to protecting your privacy and handling your personal information in an open and transparent manner. We comply with the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth).

This Privacy Policy explains how we collect, use, hold, disclose, and protect personal information when you use our website or our foreign exchange and remittance-related services.

2. Scope of This Policy

This Privacy Policy applies to:

- Visitors to our website;
- Individuals and entities who apply for or use our services; and
- Any personal information provided to us in connection with our business activities.

By providing personal information to us, you consent to its collection, use, and disclosure in accordance with this Privacy Policy.

3. Personal Information We Collect

To comply with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and other applicable laws and regulations (together, "AML/CTF Laws"), and to operate our business, we may collect and hold personal information including, but not limited to, the following:

- Identity information, such as your name, gender, date of birth, nationality, residential address, email address, contact telephone number, bank account details, identification documents, and verification information;
- Recipient or beneficiary information, including the recipient's name, date of birth, email address, residential address, bank account details, identification and verification information, and your relationship with the recipient. Recipient information is collected only where you choose to nominate a recipient or beneficiary;
- Corporate or entity client information, including business registration documents and personal information relating to directors, authorised persons, and individuals who ultimately own or control the entity;
- Transaction information and records, including information and documents generated in connection with your use of our services;
- Communications and correspondence, including any information or documents you provide to us through our website, email, phone, WeChat, WhatsApp, or other communication channels; and
- Any other information required under AML/CTF Laws, including information relating to the source of funds, purpose of transactions, or other compliance-related requirements.

Types of Personal Information Collected

Depending on the services provided, we may collect:

- Full name, date of birth, nationality and contact details;
- Residential and mailing address;
- Government-issued identification documents and verification information;
- Employment, occupation, source of funds and source of wealth information;
- Bank account details and payment information;
- Transaction records and beneficiary information;
- Politically Exposed Person (PEP), sanctions and adverse media screening results;
- Biometric information used for identity verification;
- Website, device and technical information; and
- Any other information reasonably required to provide services or comply with legal and regulatory obligations.

4. How We Collect Personal Information

How do we collect it?

In certain circumstances, we may provide additional privacy collection notices at the time personal information is collected, including where required by law or where further information is necessary to explain how your personal information will be handled.

We may collect personal information from you in the following situations:

- When you access or use our website;
- When you communicate with us by phone, email, WeChat, WhatsApp, or other messaging services;
- When you complete application forms, onboarding forms, orders, or contracts;
- When you use our services to conduct foreign exchange or remittance transactions; and
- When you otherwise voluntarily provide information to us through correspondence or other communications.

Generally, we seek to collect personal information directly from you. However, where it is reasonably necessary and lawful to do so, we may also collect personal information from third parties, including identity verification providers, banks, payment service providers, or public sources. We may also collect information from electronic identity verification providers, sanctions screening providers, fraud prevention services, government databases, and compliance technology providers where reasonably necessary to comply with AML/CTF and other legal obligations. Where required, we will take reasonable steps to notify you if we collect personal information about you from a third party.

CCTV Surveillance

If you visit our physical stores or business premises, we may collect your personal information through closed-circuit television (CCTV) systems. This may include the recording of your image and, in some cases, your voice. CCTV recordings are used for the purposes of ensuring the safety and security of our staff, customers, and property, and for the prevention, detection, and investigation of crime. Recordings are retained only for as long as reasonably necessary to fulfil these purposes, unless required or authorised by law. Where appropriate, CCTV footage may be disclosed to law enforcement or regulatory authorities in accordance with applicable laws.

5. Use of Personal Information

We collect personal information only where it is reasonably necessary for our business functions and activities. This includes providing our services, processing transactions, verifying identity, managing risk, preventing fraud, complying with AML/CTF obligations, and meeting other legal and regulatory requirements.

We may use your personal information for purposes including:

- providing our services to you;
- communicating with you, including responding to enquiries and providing transaction-related information;
- managing and administering your account or transactions;
- verifying your identity to ensure we are communicating with the correct person;
- participating in crime prevention and ensuring legal and regulatory compliance, including screening against sanctions and other compliance databases;
- conducting customer due diligence, enhanced due diligence, sanctions screening, politically exposed person (PEP) screening, and fraud prevention activities;
- monitoring transactions and customer activity to detect suspicious activity, fraud, money laundering, terrorism financing, sanctions breaches, or other unlawful conduct;
- complying with obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and related regulations.
- informing you about our products, services, or promotions that may be of interest to you, in accordance with applicable marketing and privacy laws (Customers may opt out of marketing communications at any time by using the unsubscribe facility in communications or by contacting us directly.);
- processing and administering business processes and transactions;
- monitoring, developing, and improving the quality and functionality of our services; and
- complying with applicable laws and regulatory requirements, including Australia's AML/CTF Laws and other obligations under Australian law.

6. Disclosure of Personal Information

We may disclose your personal information to third parties where it is reasonably necessary to operate our business, provide our services, process transactions, or comply with legal and regulatory obligations. In order to provide our foreign exchange and international remittance services, we may disclose your personal information to recipients located outside Australia, including overseas correspondent banks, intermediary banks, payment service providers, and beneficiary banks. This may also include payment networks, settlement systems, SWIFT messaging services, electronic verification providers, fraud prevention services, sanctions screening providers, and other service providers involved in processing, monitoring, or facilitating transactions. Overseas recipients may be located in jurisdictions including Hong Kong, China, Singapore, New Zealand, the United Kingdom, the United States, and other countries relevant to the payment instructions provided by customers.

We take reasonable steps to ensure that overseas recipients handle personal information in a manner consistent with Australian privacy standards where practicable. However, you acknowledge that some overseas recipients may not be subject to the Australian Privacy Principles under the Privacy Act 1988 (Cth).

Where required, we will obtain your express consent to such overseas disclosure as part of providing our services.

This may include disclosure to:

- our contractors or service providers who assist us in providing our services;
- intermediary or correspondent banks involved in processing transactions on your behalf;
- partners, agents, or intermediaries who are involved in providing or supporting our services;
- overseas or international intermediaries where required to complete a transaction;
- government authorities, regulators, law enforcement agencies, courts, AUSTRAC, and other entities where required or authorised by law, including for the prevention, detection, investigation, or prosecution of financial crime, money laundering, terrorism financing, sanctions breaches, fraud, or other unlawful activities.;
- our related or affiliated entities, if any.

We will never sell personal information to third parties. However, we may disclose personal information where required or authorised by law, including under the Privacy Act 1988 (Cth), other applicable legislation.

By using our services, you acknowledge that personal information may be disclosed overseas where necessary to process international transactions and that overseas recipients may not be subject to privacy laws equivalent to those in Australia.

7. Storage and Security of Information

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. We employ a combination of physical, electronic, and procedural safeguards. Security measures may include access controls, password protection, encryption, staff confidentiality obligations, secure document storage, and monitoring of system access.

Such providers may include cloud hosting, document management, email, cybersecurity, and business software providers, as part of our business systems and operational infrastructure. Access to personal information is limited to authorised employees and trusted service providers who require access to perform their duties and support the delivery of our services.

Overseas Storage and Processing

Personal information may be stored or processed by cloud service providers, software providers, and business systems located in Australia or overseas. Where personal information is transferred, stored, or processed overseas, we take reasonable steps to ensure appropriate security and privacy protections are maintained.

Data Retention

Under Australia's Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), we are legally obligated to retain certain records relating to personal identity and transactions for a minimum period of seven (7) years.

Once the applicable legal retention period has expired and the information is no longer required for any ongoing legal, regulatory, or business purpose, we take reasonable steps to securely destroy, delete, or de-identify such information.

Data Breach Notification

We comply with the Notifiable Data Breaches (NDB) scheme under the Privacy Act. In the event of a data breach that is likely to result in serious harm to any individual whose personal information is involved, we will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable after becoming aware of an eligible data breach, in accordance with our legal obligations.

8. Collection of Sensitive Information

Sensitive information may include biometric information used for identity verification, sanctions and politically exposed person (PEP) screening information, and other information collected where reasonably necessary to comply with applicable AML/CTF laws and regulatory obligations. We only collect sensitive information where permitted by law and where reasonably necessary for our business operations, risk management, or compliance requirements.

We may collect the following types of sensitive personal information:

- Biometric Information – Biometric information may include photographs, facial images, liveness checks, and other information collected through electronic identity verification providers for identity verification, fraud prevention, and compliance purposes. This may include images contained on passports, Chinese ID cards, Australian driver's licences, Chinese driver's licences, proof of age cards, Centrelink or social security cards, photo ID cards, and other government-issued identification documents.

9. Automated Decision Making

We may use automated systems to assist with identity verification, sanctions screening, fraud detection, transaction monitoring, risk assessment, and compliance reviews. Where such systems contribute to decisions that may significantly affect customers, appropriate review processes are implemented. Customers may contact us for further information regarding such decisions where permitted by law. Automated systems are used as decision-support tools and are subject to human oversight where appropriate.

Technology and Translation Tools

We may use technology tools, including document processing, translation services, fraud detection systems, identity verification technologies, and compliance systems to assist in providing our services. Where third-party technology providers are used, we take reasonable steps to ensure personal information is handled securely and in accordance with applicable privacy laws.

10. Anonymity / Pseudonym Statement

Due to AML/CTF obligations, customers generally cannot deal with us anonymously or under a pseudonym when using our financial services.

11. Cookies and Tracking Technologies

Cookies are small text files stored on your device that help support website functionality, security, and user experience. Our website may use cookies or similar technologies to analyse website usage and performance (for example, through tools such as Google Analytics), remember user preferences, and improve our services. Cookies and similar technologies may collect technical information such as IP address, browser type, device information, and interaction data. This information may constitute personal information under Australian privacy laws and may be combined with other personal information we hold. We may allow trusted third-party service providers to place cookies or use similar technologies on our website for analytical or performance-related purposes, in accordance with this Privacy Policy. You can manage, disable, or delete cookies through your browser settings. Please note that disabling cookies may affect the functionality of certain features of our website.

12. Access and Correction

You may request access to the personal information we hold about you or request correction of any personal information that you believe is inaccurate, incomplete, or outdated by contacting us using the details set out below.

To process your request, we may need to verify your identity and may ask you to specify the information you are seeking. We will acknowledge your request promptly and aim to respond within 30 days, unless a longer period is reasonably required by law.

In certain circumstances, we may be unable to provide access to some or all of your personal information, or may limit access, where permitted or required by law. These circumstances may include where:

- providing access would unreasonably affect the privacy of other individuals or organisations;
- the information is protected by legal professional privilege or relates to ongoing or anticipated legal proceedings;

- access is prohibited or restricted by law;
- providing access could reasonably be expected to pose a serious threat to the safety, physical or mental health, or life of any individual; or
- the information is commercially sensitive evaluative material.

If we refuse or limit access to personal information, we will take reasonable steps to explain the reasons for our decision, unless it would be unreasonable or unlawful to do so.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The latest version will be published on our website and will apply from the date of publication.

14. Contact Us

If you believe we have breached the Privacy Act or Australian Privacy Principles, you may lodge a privacy complaint with us in writing. We will acknowledge your complaint within 5 business days and aim to investigate and respond within 30 days.

Privacy Officer
Great International Pty Ltd
Email: compliance@greatforex.com

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC).

Website: https://www.oaic.gov.au

Phone: 1300 363 992