Web | www.doofinancial.com
US | 7700 Windrose Avenue, STE 300 Plano, Texas 75024
UK | Ground Floor, Birchin Court, 20 Birchin Lane, City of London, London, EC3V 9DU
AU | 'Tower 1' Suite 1302 Level 13, 475 Victoria Avenue, Chatswood NSW 2067, Australia.

Anti-Money Laundering and Counter-Terrorism Financing Policy

Doo Financial Australia Limited

Updated in December 2023

PART A: GENERAL

1. INTRODUCTION

1. **Doo Financial Australia Limited** (ABN: 50 100 139 820 / ACN: 100 139 820) (hereinafter referred to as the "**Doo Financial**") is an Australian financial services licensee, authorised and regulated by the Australian Securities & Investments Commission ("**ASIC**").

2. DEFINITIONS AND INTERPRETATIONS

2. The following terms shall carry the following meaning:

2.1 "Applicable Statutes and Regulations" means:

(a) statutes, rules or orders of the Relevant Regulatory Authorities;

(b) statutes, rules or orders of the relevant regulatory authorities in the client's jurisdiction;

(c) the rules of the relevant financial exchange market; and

(d) all other applicable laws to this Policy (and each as amended from time to time as applicable to this Policy).

2.2 "Board" means the director(s) of Doo Financial.

2.3 "Compliance Officer" refers to the officer appointed by the Senior Management to ensure that Doo Financial complies with all the Applicable Statutes and Regulations.

2.4 "Financial Action Task Force" or "FATF" refers to an inter-governmental policy-making body that establish and promote policies, both at national and international levels, to combat money laundering and terrorist financing.

2.5 "Politically exposed person" or "PEP" means an individual who is or has been entrusted with prominent public functions such as the Head of State, the Prime Minister, Ministers, senior politicians, senior government officials, judicial or military officials, senior executive members of state-owned corporations or international organisations and officials of a political part.

2.6 "Proceeds of crime" means property derived or realised directly or indirectly from a serious offence, including:

(i) property into which any property derived or realised directly from the offence is later successively converted or transformed; and

(ii) income, capital or other economic gains derived or realised from that property since the offence.

If property that is proceeds of crime (the original proceeds) is intermingled with other property from which it cannot readily be separated, that proportion of the whole represented by the original proceeds is taken to be proceeds of crime.

2.7 "Policy" means this Anti-Money Laundering ("**AML**") and Counter-Terrorism Financing ("**CTF**") policies and procedures;

2.8 "Proliferation financing" means the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

2.9 "Relevant Regulatory Authorities" means the relevant regulatory authority which may be applicable to Doo Financial's business operation and service providers, including but not limited to the ASIC and Australian Transaction Reports and Analysis Centre ("**AUSTRAC**").

2.10 "Senior Management" refers to any person having authority and responsibility for planning, directing or controlling the activities of Doo Financial.

2.11 "Source of wealth" refers to the origin of an individual's entire body of wealth (i.e. total assets).

2.12 "Source of funds" refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

2.13 "Terrorist financing" or "Terrorism financing" means—

(a) the provision or collection, by any means, directly or indirectly, of any property:

(i) with the intention that the property be used; or

(ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is so used);

(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate; or

(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate.

C. Purposes and Objectives of this Policy

3. Doo Financial has developed this Policy to establish the general frameworks to combat any forms of money laundering, terrorism financing or criminal activities with a strong dedication by strictly complying with the Applicable Statutes and Regulations.

4. This Policy shall cover procedures and internal controls:

(a) on the client due diligence requirements;

(b) to implement the record-keeping requirements;

(c) on the reporting requirements;

(d) to inform our officers and employees about money laundering and financing of terrorism, of the policies, processes, procedures and systems adopted by us to deal with money laundering and terrorism financing;

(e) to train our officers and employees to recognise and deal with money laundering and terrorism financing;

(f) to vet the officers and employees of Doo Financial to ensure that they are fit and proper persons to engage in anti-money laundering and counter-terrorism financing related duties;

(g) on the role and responsibility of the Compliance Officer;

(h) on the establishment of an independent audit function which can test its AML and CTF processes, procedures, and systems; and

(i) on the adoption of systems by us in dealing with money laundering and terrorism financing.

D. Commitment to this Policy

5. Doo Financial has established a series of AML procedures and will apply the AML and Know-Your-Client ("**KYC**") procedures in all transactions.

5.1 We are committed to taking all reasonable measures to ensure that proper protection exists to prevent a contravention of the Applicable Statutes and Regulations in fending off and mitigating money laundering and terrorism financing ("**ML and TF**") activities.

5.2 Compliance with the AML and CTF system has always been our utmost priority to preserve our business reputation in the global financial industry and regulatory authorities. We will require all of our employees, agents, representatives, contractors and any other related person representing Doo Financial to strictly adhere to this Policy to detect and prevent our services and/or products being used for ML and TF activities.

5.3 In the event a MT and TF activity is reported and/or discovered, we are committed to take immediate and necessary actions against the individual or group engaging in the MT and TF

activity. This shall include filing a report to the Relevant Regulatory Authorities as required and stated in this Policy below.

5.4 In the event any of our employees, agents, representatives, contractors and any other related person representing Doo Financial is found to be in breach and/or non-compliance with this Policy, Doo Financial will investigate and, depending on the nature of the breach and/or non-compliance, may result in further training, termination of employment, termination of agency, revocation of authorization, or other disciplinary or punitive action.

6. POLICY AUDIT FUNCTION

6.1 The Compliance Officer and our compliance department will conduct an internal audit on this Policy annually to ensure that it is updated. We are aware of our statutory responsibility to comply with the Applicable Statutes and Regulations, and we shall update and review this Policy at least once annually.

6.2 We adopt a risk-based approach in the implementations of our AML and CTF systems and for the purpose of detecting ML and TF risks. We update our AML and CTF systems and the Policy at least once annually to take into account any new and emerging risks, considering:

(a) the nature and level of money laundering and terrorism financing risk that we may reasonably expect to face in the course of its business;

(b) the nature, size and complexity of our business;

(c) development of new products and new business practices, including new delivery mechanisms; and

(d) use of new or developing technologies for both new and pre-existing products.

7. EMPLOYEE SCREENING OR DUE DILIGENCE PROGRAMME

7.1 Doo Financial will carry out the following due diligence procedures on every employee prior to them being employed and/or involved in any AML and CTF related matters. The due diligence check includes but not limited to:

(a) identity documents, such as passport, identity card, driving licence, and other relevant documents;

(b) employment reference;

(c) academic qualification check;

(d) professional recognition check (if applicable);

(e) right to work in Australia (if the employee is not an Australian);

(f) bankruptcy check; and

(g) criminal history check;

(h) ASIC Disqualified Person check.

7.2 The results of the screening or due diligence processes are to be maintained and kept for a period of seven (7) years from the date of their employment with Doo Financial.

7.3 Doo Financial shall re-screen all the employees every three (3) years. In the case of the Compliance Officer and other employees in the compliance department, the screening or due diligence will be conducted on annual basis.

8. EMPLOYEE TRAINING AND AWARENESS PROGRAMME

8.1 In order to ensure that all employees in Doo Financial are aware of this Policy, they will be:

(a) provided with relevant policy and knowledge training as contained and provided in this Policy;

(b) briefed about their job descriptions;

(c) trained on their responsibilities concerning money laundering and financing of terrorism transactions; and

(d) guided on how to identify and deal with transactions that possibly involve money laundering and financing of terrorism.

8.2 Scope of training

8.2.1 Staff will be made aware of:

(a) the statutory obligations and the possible consequences for failure to report suspicious transactions under the Applicable Statutes and Regulations;

(b) any other statutory and regulatory obligations that concern us under the Applicable Statutes and Regulations, and the possible consequences of breaches of these obligations;

(c) our policies and procedures relating to AML and CTF, including suspicious activity and transaction identification and reporting;

(d) any new and emerging techniques, methods and trends in ML and TF to the extent that such information is needed by the staff to carry out their respective roles concerning AML and CTF;

(e) escalation procedures, i.e. what to do once a ML and TF risk is identified;

(f) what the staff's role is in our compliance's efforts and how to perform them;

(g) record keeping and record retention policy; and

(h) disciplinary consequences (civil and criminal) for non-compliance with the Applicable Statutes and Regulations.

8.2.2 Focused training for appropriate staff or groups of staff will enable Doo Financial and senior management to implement their AML and CTF systems effectively. The following areas of training may be appropriate for certain groups of staff:

(a) All new staff (irrespective of seniority)

(i) an introduction to the background of ML and TF and the importance of AML and CTF to Doo Financial; and

(ii) the need and obligation to identify and report suspicious transactions to the Compliance Officer, and the offence of "tipping-off".

(b) Front-line staff (i.e. staff dealing with clients directly)

(i) the importance of their roles in the Doo Financial's AML and CTF strategy being the first point of contact with potential money launderers and persons involved in TF;

(ii) the Doo Financial's policies and procedures in relation to Client Due Diligence ("**CDD**") and record-keeping requirements relevant to their job responsibilities;

(iii) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and

(iv) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be required.

(c) Back-office staff

(i) appropriate training on client verification and the relevant processing procedures; and

(ii) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.

(d) Managerial staff (including internal audit staff)

(i) higher-level training covering all aspects of AML and CTF regime;

(ii) specific training in the AML and CTF requirements applicable to us; and

(iii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as the reporting of suspicious transactions to the Relevant Regulatory Authorities.

(e) Officer

(i) specific training in relation to the Officer's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the Relevant Regulatory Authorities;

(ii) training to keep abreast of AML and CTF requirements/developments generally;

(iii) receive reports of suspicious activity from firm personnel; and

(iv) coordinate required AML reviews/meetings with appropriate staff.

8.3 We will monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of our policies and procedures to combat ML and TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions;

(b) monitoring the staff's compliance with our AML and CTF systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken; and

(c) monitoring attendance and following up with staff who miss such training without reasonable cause.

8.4 We conduct AML training, workshops and assessments on all related staff members at least once annually.

8.5 We shall observe and record our employees who have been adequately trained, when they are trained or last trained, and thereafter provide additional, necessary and adequate training to them.

9. RECORD KEEPING

9.1 Records of all original and/or copy of documents, including but not limited to, identity verification documents, transaction records, CDD information, ML and TF reports, all documents submitted in relation to suspicious activity, suspicious transaction, results of the suspicious transaction report and other related documents shall be compiled and organized with confidentiality for at least seven (7) years from the date of creation of the said documents.

9.2 The record-keeping requirements in respect of each client are as follows:

(a) We must keep the original and/or a copy of:

(i) the documents, and a record of the data and information obtained in the course of identifying and verifying the identity of the client, beneficial owner of the client, and the person who purports to act on behalf of the client (if any); and

(ii) the documents in relation to the client's business relationship, any beneficial owner of the client, and business correspondences with the client; and

(b) The documents and records mentioned in sub-paragraph (a) above must be kept throughout the continuance of the business relationship with the client and for at least seven (7) years following the termination of the business relationship.

9.3 The record keeping requirements in respect of each transaction are as follows:

(a) We will keep the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, including but not limited to the following:

(i) nature of the transaction;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted;

(iv) the name, address and occupation, business or principal activity, as the case requires, of each person:

(aa) conducting the transaction; and

(ab) for whom, or for whose ultimate benefit, the transaction is being conducted, if we have reasonable grounds to believe that the person is undertaking the transaction on behalf of any other person;

(v) the type and identifying number of any accounts/services with us that were involved in the transaction;

(vi) if the transaction involves a negotiable instrument other than currency:

(aa) the drawer of the instrument;

(bb) the name of the institution on which it is drawn;

(cc) the name of the payee (if any);

(dd) the amount and date of the instrument; and

(ee) the number (if any) of the instrument and details of any endorsements appearing on the instrument;

(vii) the name and address of Doo Financial, and of each officer, employee, or agent of Doo Financial who prepared the relevant record or a part of the record; and

(viii) any other information relating to that transaction.

(b) Records required to be kept under subparagraph (a) must be kept for at least seven (7) years following the completion of the transaction, regardless of whether the business relationship ends during the period.

10. ROLES AND RESPONSIBILITIES

10.1 General

9.1.1 The Board, Senior Management and Compliance Manager of Doo Financial are obliged to oversee and administer the implementation of this Policy. Their respective roles and responsibilities are outlined in this Policy below.

10.2 Board

9.2.1 The Board must be cognizant of the ML and TF risks associated with business strategies, delivery channels and geographical coverage of Doo Financial's products and services.

9.2.2 The Board has the following roles and responsibilities:

(a) to maintain accountability and oversight for establishing AML and CTF policies and minimum standards;

(b) to review the policies regarding AML and CTF measures within Doo Financial, including but not limited to record keeping, CDD, on-going due diligence, risk assessment, and reporting systems.

(c) to review and approve an effective internal control system for AML and CTF;

(d) to maintain adequate oversight of the overall AML and CTF measures undertaken within Doo Financial;

(e) to ensure effectiveness of the internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML and TF; and

(f) to evaluate and appraise the implementation of the AML and CTF policies through regular reporting and/or updates by the Senior Management and/or Compliance Officer.

10.3 Senior Management

10.3.1 Senior Management is accountable for the implementation and management of this Policy in accordance with the policies and procedures established by the Board, industry's standards and best practices, and the Applicable Statutes and Regulations.

10.3.2 The Senior Management has the following roles and responsibilities:

(a) to be aware of and understand the ML and TF risks associated with the business strategies, delivery channels and geographical coverage of Doo Financial's products and services offered and to be offered.

(b) to formulate this Policy to ensure that it is in line with the risks profiles, nature of business, complexity, volume of the transactions and geographical coverage of Doo Financial;

(c) to establish appropriate mechanisms and formulate procedures to effectively implement this Policy and internal control system approved by the Board;

(d) to review and propose to the Board the necessary enhancements to this Policy to reflect changes in the business strategies, delivery channels and geographical coverage of Doo Financial's products and services;

(e) to allocate adequate resources to effectively implement and administer this Policy;

(f) to ensure that all AML and CTF related issues raised are addressed in a timely manner; and

(g) to ensure the integrity of the employees by establishing appropriate employee screening or due diligence system.

10.4 Compliance Officer

10.4.1 The Compliance Officer acts as the reference point for AML and CTF related matters within the Doo Financial. The Compliance Officer must possess the necessary knowledge and expertise to keep abreast with the latest developments of AML and CTF measures in the industry that may affect the business of Doo Financial.

10.4.2 The Compliance Officer has the following roles and responsibilities:

(a) to ensure the compliance with the AML and CTF requirements;

(b) to ensure the proper implementation of this Policy and the internal control system;

(c) to report to and liaise with the Board and/or Senior Management on all AML and CTF related matters;

(d) to amend and update this Policy in accordance with the recommendations from the Board and Senior Management;

(e) to effectively implement all the AML and CTF measures within Doo Financial, including but not limited to record keeping, CDD, on-going due diligence, risk assessment, and reporting systems;

(f) to regularly assess the AML and CTF mechanisms such that it is effective and sufficient to address any change in the ML and TF trends;

(g) to identify the possible ML and TF risks associated with the new products and/or services to be provided by Doo Financial;

(h) to provide appropriate levels of AML and CTF trainings to all staff at all levels within Doo Financial;

(i) to ensure that all staff in Doo Financial are aware of AML and CTF measures, control mechanism and reporting channels within this Policy;

(j) to review all internal reports of suspicious transactions and exception reports and, in the light of all available information, determine whether or not it is necessary to file a suspicious activity report or suspicious transaction report with the Relevant Regulatory Authorities;

(k) to maintain all records relating to the internal reviews of suspicious transactions and exception reports;

(l) to comply with any other obligations that are imposed under this Policy.

10.4.3 Notwithstanding Clause 9.4.2 above, the Compliance Officer shall be responsible for reporting any feedback received from AUSTRAC to the Board, Senior Management and compliance department. Subsequently, the Compliance Officer shall ensure that appropriate follow up actions are initiated, taken and implemented.

11. Money Laundering

11.1 The stages of money laundering are as follows:

(i) Placement - disposal of cash proceeds derived from illegal activities;

(ii) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(iii) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

11.2 Some of the possible signs of money laundering includes, but is not limited to the following:

(i) reluctance by clients to provide information;

(ii) incomplete or inconsistent information by clients;

(iii) irregular money transfers and transactions;

(iv) unexplained third-party investment;

(v) transactions carried by unusually high volume;

(vi) source of funds from poorly-regulated sources;

(vii) transactions with no apparent legitimate or economic purpose;

(viii) transactions which are unnecessarily complex;

(ix) client's lifestyle appears in excess of known sources of income;

(x) business structure is unnecessarily complicated;

(xi) use of bank accounts without valid reason;

(xii) the client appears to be acting as an agent for another entity or individual but is evasive about the identity of another identity;

(xiii) the client has multiple accounts under a single name or multiple names, with a large number of inter-account transfers; and

(xiv) the client deposit funds followed by a request to withdraw the funds.

PART B: KNOW-YOUR-CLIENT ("KYC")

12. PURPOSE AND OBJECTIVE

12.1. Doo Financial has established this KYC policy to set out the guidelines and procedures for the verification of all our clients' identities.

12.2. Doo Financial shall verify and be satisfied with the identity of the following through reliable and independent documentation, electronic data and/or other measures as deemed necessary:

(a) the client;
(b) the beneficial owner of the client (if any); and
(c) a person acting on behalf of the client (if any).

12.3. Doo Financial shall carry out the identity verification procedure before providing a designated service for or establishing a business relationship with the client.

13. CLIENT DUE DILIGENCE ("CDD")

13.1. Doo Financial performs on-going due diligence process to monitor our client's account, service or relationship with each of our clients to identify, mitigate and manage the risk it may reasonably face with its client that might involve money laundering, financing of terrorism or other serious offences.

13.2 Doo Financial performs CDD if a person:

(a) opens an account with us;

(b) engages our services; or

(c) enters into a business relationship with us.

13.3 Doo Financial performs CDD on:

(a) a person conducting a transaction;

(b) a person on whose behalf a transaction is being conducted; and

(c) a beneficial owner;

if we have reasonable grounds to believe that the person is undertaking a transaction on behalf of another person. We shall verify whether such a person is authorised to undertake the transaction concerned on behalf of the other person.

13.4 Furthermore, we carry out CDD on the client:

(a) before establishing a business relationship with the client;

(b) when we are requested by Relevant Regulatory Authorities, payment service providers or service providers to perform appropriate CDD;

(c) when we carry out an electronic currency transfer for the client;

(d) when we suspect that the client is involved in proceeds of crime, financing of terrorism or a serious offence regardless of the levels of transaction in Clause 11.4(b) above;

(e) when we suspect that the client's source of funds originated from a third party;

(f) when we suspect that the transaction involves proceeds of crime, or may be used for financing terrorism or for committing a serious offence;

(g) when we have doubts on the veracity or adequacy of the client identification or information it had previously obtained; or

(h) when we are performing our regular CDD routine.

13.5 **Required document list**

13.5.1 If the client is an individual, we shall collect the following information:

(a) the client's full name;

(b) the client's date of birth;

(c) the client's residential address;

(d) the client's occupation;

(e) the client's country(ies) of citizenship;

(f) the client's country(ies) of residence;

(g) the client's occupation or business activities;

(h) the nature and purpose of the client's proposed relationship with us, including:

(i) the purpose of specific transactions; or

(ii) the expected nature and level of transaction behaviour;

(i) authorization of any person purporting to act for or on behalf of the client;

(j) the income or assets available to the client;

(k) the client's source of funds including the origin of funds;

(l) the client's financial position;

(m) the beneficial ownership of the funds used by the client; and

(n) the beneficiaries of the transactions being facilitated by us on behalf of the client including the destination of funds.

13.5.2 If the client is a foreign registered body corporate, we shall collect the following information:

(a) full name of the foreign company;

(b) the country of registration and full registration detail of the client;

(c) the full address of the company's principal place of business and registered address;

(d) the company structure;

(e) name of each company director and secretary;

(f) nature of the business activities conducted by the company;

(g) name and address of beneficial owners of the company and the control structure;

(h) the country in which the company was formed, incorporated or registered;

(i) the provisions regulating the power to bind the client;

(j) the authorization of any person purporting to act for or on behalf of the client, and the identity of the persons; and

(k) the purpose and intended nature of the business relationship with us.

13.6 We strictly prohibit establishing any business relationship with clients with false, fictitious or misleading names, and we shall make a record of if any of our client is using a different name from which the client is commonly known.

13.7 We will consider on a case by case basis any clients that cannot reasonably be expected to produce the standard evidence of identity and will seek to agree on the use of other confirmations of identity so that clients are not unreasonably denied access to the products and services. In the event it is reasonably proved that there is doubt on the identification and verification of the beneficial owners, we may carry out CDD on the senior management officials of the client in accordance with this AML and CTF policy.

14. CLIENT RISK ASSESSMENT ("CRA")

14.1 Doo Financial will perform CRA using the risk-based approach. We assess the risk for each client taking into account specific products, services, clients, entities, number of transactions, volume of transactions, nature of client relationships, geographic locations, the purpose of the account or relationship, the level of assets involved, the size of transactions to be undertaken and the regularity or duration of the business relationship.

14.2 We will not accept high-risk clients that are identified as follows:

a. clients with business that handles a large amount of cash or complex unusually large transactions, which could not be verified.

b. clients with large one-off transactions, or several transactions carried out by the same account within a short time.

c. clients based in or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime, weapon or drug production, distribution, stockpiling or acquisition.

d. clients falling under the definition of PEP.

e. Transactions with the source funds that cannot be verified.

f. Transactions with no apparent economic or legitimate purpose.

g. Transactions that might favour anonymity.

14.3 We will conduct a client risk assessment at the initial stage of CDD to determine the extent of CDD measures and ongoing monitoring measures to be applied. We subsequently take a risk-based approach and conduct ongoing monitoring of business relationships with clients to manage and mitigate money laundering and terrorism financing risks, and ensure all related information are updated. The client risk assessment framework shall be proportional to the nature and size of Doo Financial's business with clients.

14.4 When we have any reasonable grounds of suspicion, the client will be required to identify and verify the source or destination of the transactions.

14.5 Our steps to conduct the institutional money laundering/terrorism financing risk assessment include:

(a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis and information obtained from relevant internal and external sources;

(b) considering all the relevant risk factors before determining the level of overall risk, and the appropriate level and type of mitigation to be applied;

(c) obtaining the approval of senior management on the risk assessment results;

(d) having a process by which the risk assessment is kept up-to-date; and

(e) having appropriate mechanisms to provide the risk assessment to the Relevant Regulatory Authorities when required to do so.

15. SIMPLIFIED DUE DILIGENCE ("SDD")

15.1 If Doo Financial has determined that ML and TF risks are low, Doo Financial may adopt a simplified due diligence ("SDD") approach.

15.2 clients to whom SDD may be applied are:

(a) a financial institution;

(b) an institution that:

(i) is incorporated or established in an equivalent jurisdiction;

(ii) carries on a business similar to that carried on by a financial institution;

(iii) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the regulatory authorities;

(c) a corporation listed on any stock exchange;

(d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is:

(i) a financial institution;

(ii) an institution incorporated or established which:

- has measures in place to ensure compliance with requirements similar to those imposed in the Applicable Statutes And Regulations; and
- is supervised for compliance with those requirements.

(e) the government or any public body; or

(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

15.3 In cases of SDD, we will:

(a) identify the client and verify the client's identity;

(b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with us; and

(c) if a person purports to act on behalf of the client,

(i) identify the person and take reasonable measures to verify the person's identity; and

(ii) verify the person's authority to act on behalf of the client.

16. ENHANCED DUE DILIGENCE ("EDD")

16.1 If Doo Financial has determined that ML and TF risks are high, Doo Financial shall adopt an enhanced due diligence ("EDD") approach and enhanced ongoing monitoring. Approval from the Senior Management will be required before engaging or continuing a business relationship and/or transaction with high risks clients.

16.2 High-risk situations for which EDD apply includes:

(a) client risk factor:

(i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between us and the client);

(ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;

(iii) companies that have nominee shareholders or shares in bearer form;

(iv) cash-intensive business;

(v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business; or

(vi) the client or the beneficial owner of the client is a PEP or foreign PEP.

(b) product, service, transaction or delivery channel risk factors:

(i) anonymous transactions (which may involve cash); or

(ii) frequent payments received from unknown or non-associated third parties.

(c) country risk factors. We strictly prohibit all dealings, bank transfers and transactions with clients from high risk countries, including but not limited to:

(i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML and CTF systems;

(ii) countries identified by the Financial Action Task Force;

(iii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

(iv) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or

(v) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.

16.3 Doo Financial reserves the right to obtain information from our independent source for enhanced due diligence measures. This includes but is not limited to:

(a) obtaining additional information on the client (e.g. occupation, volume of assets, ownership and control structure, client's or beneficial owner's reputation, information available through public databases, internet, etc.), and updating more regularly the identification data of the client and beneficial owner;

(b) obtaining additional information on the intended nature, purpose and background of the business relationship and transactions;

(c) obtaining information on the source of funds or source of wealth of the client;

(d) obtaining information on the reasons for intended or performed transactions; and/or

(e) requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

16.4 Our EDD entails:

16.4.1 **Increasing the quantity of information obtained for client due diligence purposes:**

(a) About the client's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the client's or beneficial owner's reputation and assessing any negative allegations against the client or beneficial owner. Examples include: information about family members and close business

partners; information about the client's or beneficial owner's past and present business activities; and adverse media searches;

(b) About the intended nature of the business relationship, to ascertain whether that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete client risk profile. It includes obtaining information on:

(i) the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate;

(ii) the reason the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction;

(iii) the destination of funds;

(iv) the nature of the client's or beneficial owner's business to understand the likely nature of the business relationship better.

16.4.2 **Increasing the quality of information obtained for client due diligence purposes to confirm the client's or beneficial owner's identity including by:**

(a) Requiring the first payment to be carried out through an account verifiable in the client´s name with a bank;

(b) Establishing that the client's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with our knowledge of the client and the nature of the business relationship. The sources of funds or wealth may be verified, among others, by reference to income tax returns, copies of audited accounts, payslips, public deeds or independent and credible media reports;

(c) Increasing the frequency of reviews, to be satisfied that we continue to be able to manage the risk associated with the individual business relationship and to help identify any transactions that require further review, including by:

(i) Increasing the frequency of reviews of the business relationship, to ascertain whether the client's risk profile has changed and whether the risk remains manageable;

(ii) Obtaining the approval of the Officer/nominated officer to commence or continue the business relationship to ensure senior management are aware of the risk we are exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

(iii) Reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon;

(iv) (iv) Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorism financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions;

(d) The Compliance Officer will need to provide approval, or refusal, to proceed with the client set up process before conducting any business with a client who has been through the enhanced due diligence process.

16.5 We will apply EDD measures on any situations, clients or transactions that are deemed to be high risk by us.

16.6 **Source of Funds and Source of Wealth**

14.6.1 Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets).

14.6.2. Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

16.7 **How Source of Funds and Source of Wealth measures are incorporated into our EDD Process**

16.7.1 Source of wealth will usually indicate the size of wealth the client would be expected to have, and a picture of how the individual acquired such wealth. Although we may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

16.7.2 Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

16.8 Doo Financial shall not accept any funding from any third party, but in the event such exceptional circumstances occur, we shall conduct EDD to identify and verify its ultimate beneficial owner including legal person, partnership, trust and other legal arrangements.

17. VERIFICATION

17.1 We shall verify and screen the client's information above through our client service and risk management department. Our scope of CDD includes, but is not limited to our retail clients, business partners, the board members, shareholders and ultimate beneficial owner. We carry out the following CDD measures:

(a) identify, verify and screen the client's identity and information via an independent screening system;

(b) where there is a beneficial owner in relation to the client, identifying and taking reasonable measures to verify the beneficial owner's identity so that we are satisfied that we know who the beneficial owner is, including in the case where the client is a legal person or trust, measures to enable us to understand the ownership and control structure of the legal person or trust;

(c) obtaining information on the purpose and intended nature of the business relationship (if any) established with us unless the purpose and intended nature are obvious; and

(d) if a person purports to act on behalf of the client:

(i) identifying the person and taking reasonable measures to verify the person's identity using documents, data or information provided by reliable and independent source; and

(ii) verifying the person's authority to act on behalf of the client;

(e) if we deem the identity verification insufficient or if we require additional details relevant to the transaction performed by the client, we reserve the right to request additional details from the client (including but not limited to bank statement, proof of bank account, electronic wallet or electronic currency statement) and reserve our right not to establish a business partnership or proceed with any further transaction. If the client either refuses to provide the required information, or provide false/misleading information, we may freeze the client account, restrict trading or account activity, terminate the business partnership and/or report to the regulatory authority. Upon satisfactory verification of the client's identity and the transaction details, all restrictions applied on the account shall be lifted.

17.2 In the identity verification process, we will request a copy of the original and a coloured scanned copy of the identification documents; we may also request more than one identity documents for cross-verification if we deem necessary.

17.3 When electronic verification is used or a client has not been physically present for identification purposes, we will carry out an additional verification check to manage the risk of impersonation fraud. This check may take the form of:

(a) requiring the first payment to be carried out through an account in the client's name with a regulated credit institution;

(b) telephone contact with the client on a home or business number that has been verified, before opening the account;

(c) communicating with the client at the address that has been verified;

(d) requiring copy documents to be certified by an appropriate person.

17.4 If we are unable to carry out the prescribed identification process on a person, we:

(a) shall not open an account for the person;

(b) shall not enter into a business relationship with the person; and

(c) if a business relationship already exists with the person, we shall terminate the existing business relationship.

18. REPORT

18.1 If satisfactory evidence of the identity or verification of a person is not produced to or obtained by us within 14 working days (2 working days if Clause 11.4(d) and (e) arise), we shall submit a suspicious activity report to the Relevant Regulatory Authorities. We shall not proceed any further with the transaction unless directed to do so by the Relevant Regulatory Authorities.

18.2 In the event we suspect on reasonable grounds that the client is not the person that he or she claims to be, we shall take one or more of the actions below within 3 working days commencing after the day on which the circumstance comes into existence:

(i) collect the necessary client identification information in respect of the client; or

(ii) verify, from a reliable and independent source, certain client information that has been obtained in respect of the client; to ensure it is reasonably satisfied that the client is the person that he or she claims to be.

18.3 When determining and putting in place appropriate risk-based systems and controls, we shall consider the nature, size and complexity of the client's business and type of ML and TF risks that we might reasonably face, including but not limited to the following factors:

(a) client types, including PEPs;

(b) the types of designated services provided;

(c) method by which we deliver designated services, including any development of new products, business practices and use of new or developing technologies;

(d) the foreign jurisdictions with which we deal, including high risk jurisdictions as identified by Financial Action Task Force.

18.4 If any of the following events occurs:

(a) suspicious transaction;

(b) suspicious activity;

(c) transaction conducted by money laundering entities;

(d) transaction involving terrorist property;

(e) transaction with no legitimate purpose;

(f) our supervisory body or auditor has reasonable grounds to suspect that a transaction or an attempted transaction or information that it has in its possession involves proceeds of crime or is related to the financing of terrorism; or

(g) any transaction described in Clause 10.2;

the transaction should be suspended and should not proceed without the authorization of the Officer. Our frontline staff shall report any suspicious transaction or activity without delay to the Officer, who will then make a suspicious activity or suspicious transaction report to the Relevant Regulatory Authorities in 2 working days if required.

18.5 If suspicious signals of money laundering are identified, the transaction should be suspended and should not proceed without the authorization of the Officer. After making appropriate investigations, the Officer will report the matter to the Relevant Regulatory Authorities if we believe there is any potential serious ML and TF risks. In the event we deem a person conducts 2 or more transactions with the intention to avoid the amount threshold as described in Clause 11.4(b), we shall submit a suspicious transaction report to the Relevant Regulatory Authorities. We shall consider the following factors before submitting our report:

(a) the manner and form in which the transactions were conducted;

(b) the amount of the currency involved in each transaction;

(c) the aggregate amount of the currency involved in the transactions;

(d) the period over which the transactions occurred;

(e) the interval of time between the transactions;

(f) the locations at which the transactions were initiated or conducted;

(g) any explanation made by the person concerned as to the manner or form in which the transactions were conducted.

18.6 **Procedure of handling suspicious activity report and suspicious transaction report**

18.6.1 After making appropriate investigations, the Officer will consider, if appropriate, reporting the matter to the regulatory authority. All records to the Officer and the relevant authorities, shall be kept by the Officer for a term of no less than 7 years after the matter has been closed by the regulatory authority. The suspicious activity report or suspicious transaction report shall include:

(a) personal particulars and contact details of the individuals or entities involved in the suspicious activity or transaction;

(b) details of the suspicious activity or transaction;

(c) the suspicious activity or transaction indicators observed; and

(d) any explanation provided by the subject of the suspicious activity report or suspicious transaction report when questioned about the transaction or activity.

18.6.2 The filing of a suspicious activity report or suspicious transaction report to the Relevant Regulatory Authorities provides us a statutory defence to the offence of ML and TF in respect of the acts disclosed in the report, provided that:

(a) the suspicious activity report or suspicious transaction report is made before we undertake the disclosed acts and the acts or transactions are undertaken with the consent of the Relevant Regulatory Authorities; or

(b) the suspicious activity report or suspicious transaction report is made after we have performed the disclosed acts or transactions and the report is made on our initiative and as soon as it is reasonable for us to do so.

18.7 All notifications made will be handled with strict confidentiality. However, please note that there may be circumstances in which we are required to reveal an individual's identity, for example where we are compelled to do so by law and therefore anonymity cannot be guaranteed.

18.8 We are aware that it is an offence for a person, knowing or suspecting that a disclosure has been made to the Relevant Regulatory Authorities, if he/she discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off"). The client's awareness of a possible suspicious activity report or suspicious transaction report or investigation could prejudice future efforts to investigate the suspected ML and TF operation. Therefore, if we form a suspicion that transactions related to ML and TF, we will take into account the risk of tipping-off when performing the CDD process. We shall ensure that our employees are aware of and sensitive to these issues when conducting CDD.

18.9 We shall not disclose any information to any other person:

(a) that we, or our supervisory body or auditor or a person has formed a suspicion in relation to a transaction or an attempted transaction, or an activity or attempted activity; or

(b) that a report under Applicable Statutes And Regulations is made to Relevant Regulatory Authorities; or

(c) that information under the Applicable Statutes And Regulations is given to Relevant Regulatory Authorities; or

(d) any other information from which a person to whom the information is disclosed may reasonably be expected to infer any circumstances in paragraph (a)-(c).

18.10 Clause 18.9 does not apply to a disclosure made to:

(a) an officer, employee or agent of a Doo Financial who has made or is required to make a report or provide information under this Applicable Statutes And Regulations for any purpose connected with the performance of that our duties; or

(b) a lawyer for the purpose of obtaining legal advice or representation in relation to the disclosure; or

(c) the supervisor of Doo Financial; or

(d) a law enforcement agency or any other person assisting the Relevant Regulatory Authorities under this Applicable Statutes and Regulations.

19. ONGOING CDD AND TRANSACTION MONITORING

19.1 We shall conduct ongoing monitoring through ongoing CDD and transaction monitoring to ensure compliance with the AML and CTF Systems. We shall review the existing CDD records upon any trigger events and maintain adequate systems to monitor transactions in accordance with the risk-based approach adopted. The extent of monitoring shall be proportional to the ML and TF risk profile of a client.

19.2 Ongoing CDD

19.2.1 We continuously monitor the activity of our clients by:

(a) reviewing from time to time documents, data and information relating to the client that have been obtained to comply with CDD requirements to ensure that they are up-to-date and relevant;

(b) conducting appropriate scrutiny of transactions carried out for the client to ensure that they are consistent with our knowledge of the client and the clients' business, risk profile and source of funds; and

(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate ML and TF.

19.2.2 All clients that present high ML and TF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by us, to ensure the CDD information retained is consistent with our knowledge of the client, the client's business, source of funds and risk profile.

19.2.3 On an annual basis, all clients, who have been classed as high risk, will undergo a complete review. This will entail establishing the following:

(a) Re-confirmation of address

(b) Re-confirmation of corporate structure (if applicable)

(c) Re-confirmation of Source of Funds and Wealth

(d) Screening for adverse news

(e) Complete review of transaction profile, including new products requested

17.3 Transaction monitoring

17.3.1 We maintain adequate systems to monitor and review all transactions performed based on a risk-based approach, and we shall check and review whether the transactions are normal based on the following factors:

(a) the size and complexity of its business;

(b) the ML and TF risks arising from its business;

(c) the nature of its systems and controls;

(d) the monitoring procedures that already exist to satisfy other business needs; and

(e) the nature of the products and services provided (which includes the means of delivery or communication).

17.3.2 We regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds adopted include the following factors:

(a) the nature and type of transactions (e.g. abnormal size or frequency);

(b) the nature of a series of transactions (e.g. structuring a single transaction into several cash deposits);

(c) the counterparties of transactions;

(d) the geographical origin/destination of a payment or receipt;

(e) the client's normal account activity or turnover;

(f) the client's behaviour - sudden and/or significant changes in transaction activity by value, volume or nature, such as change in beneficiary or destination;

(g) client's linked relationships – identifying common beneficiaries and remitters amongst apparently unconnected accounts or clients.

17.3.3 We will carry out retrospective reviews on the client to ensure the business being transacted is consistent with what was anticipated when the client was taken in. The frequency will depend on the risk classification of the client:

(a) high risk will be reviewed no less than weekly;

(b) medium risk will be reviewed no less than monthly;

(c) low risk will be reviewed on a real-time risk basis and may not need to undergo a retrospective check.

18. AML AND CTF SCREENING PROCESS

18.1 We strictly prohibit clients related to terrorism financing, proliferation financing, PEP and clients on the financial sanctions list decided by the UN Security Council. We shall not conduct any business relationship with them in any way.

18.2 We screen:

(a) clients and any beneficial owners of the clients against the current database at the establishment of the relationship;

(b) clients and any beneficial owners of the clients against all new and any updated designations to the database as soon as practicable; and

(c) all relevant parties in a cross-border wire transfer against the current database before executing the transfer;

(d) against the latest list of designated individuals and entities extracted from sanction lists published by international regulatory authorities.

18.3 In case of any suspicions of terrorism financing, proliferation financing and sanctions violations, we will submit a suspicious activity or suspicious transaction report to the Relevant Regulatory Authorities. We will report any asset frozen or actions taken in compliance with the financial sanctions requirements by way of filing a suspicious activity report or suspicious transaction report to the Relevant Regulatory Authorities.

19. LANGUAGE AND AMENDMENTS

19.1 The official language of this AML and CTF policy shall be English. Doo Financial may provide this AML and CTF policy in other languages for information purposes only and in the event of any inconsistency or discrepancy between the English version of this AML and CTF policy and any other language version, the English version shall prevail.

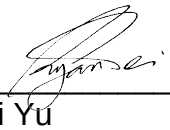
19.2 The client acknowledges that Doo Financial reserves the right to amend or update this AML and CTF policy at any time without prior notice to the client. The amendments to the AML and CTF policy shall become effective immediately and shall be legally binding on the client upon publishing of the AML and CTF policy on Doo Financial's website. The client undertakes to regularly review this AML and CTF policy on the Doo Financial's website.

(the rest of this page is intentionally left blank)

Signed by the Board of Doo Financial Australia Limited (or by their agent):

Junjie Chen

Guofei Chen



Pei Yu

Date: 15th December 2023