Anti- Money Laundering (AML)/ Know Your Customer (KYC) Policy

TF Global Markets (Aust) Pty Ltd holder of Australian Financial Services Licence (AFSL) number 424700. ABN: 69158361561.

Derivative Issuer Licence issued by the Financial Markets Authority in New Zealand Financial Service Provider (FSP623289)

TF GLOBAL MARKETS (AUST) PTY LTD

Baker Tilly Staples Rodway Auckland Ltd, 9th Floor, 45 Queen Street, Auckland, 1010, NZ.

+64 3 668 4583

Table of Contents

1. Purpose

The primary purpose of this policy is to set out the customer identification procedures for different types of customers and designed to meet any requirements set out under the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act).

2. Background

This policy sets out procedures for different types of:

- customers;
- services; and
- circumstances.

This procedure consists of risk-based systems and controls, appropriate to the nature, size, and complexity of our business, and prepared considering the risk that we face that we will be involved in or facilitate money laundering (ML) or terrorism financing (TF).

3. Identifying customers

Customers include individuals, companies, trusts and partnerships.

Before we provide a designated service to the customer for the first time (even when we have provided services to the customer in the past), we collect information about the customer. We are prohibited from providing our services to the customer until the customer identification procedures have been carried out.

We collect information about a customer from a third party because it is unreasonable or impractical to collect the information from the customer, and it is reasonably necessary for our functions or activities.

We use the onboarding forms as set out in Annexure D to collect information about each customer in accordance with their customer type.

Before we provide a designated service to the customer for the first time (even when we have provided services to the customer in the past), we also categorise customers into a certain risk category. That categorisation will determine what needs to be identified and verified.

Annexure B sets out an explanation of how the Customer Risk Assessment Tool (Annexure C) is used.

Our customer risk assessment process is outlined in Annexure B. The risk rating assigned to a customer will affect the KYC information and procedures which are applied to that customer. The minimum customer identification and verification checks that we conduct for each customer type are set out in Annexure D. Additional KYC checks are conducted on customers assessed as high ML/TF risk. We implement additional checks for high-risk customers for each customer type.

Applicants complete and submit an online form to create an account and are required to provide a valid e-mail address not present already in our system, their personal and financial details, their trading experience, and a password of their choice.

If we suspect on reasonable grounds that the customer is not who they claim to be, within 14 days we will do at least one of:

1. collect any KYC information in respect of the customer; or
2. verify, from a reliable and independent source, KYC information that has been obtained in respect of the customer,

to enable us to be reasonably satisfied that the customer is the person they claim to be.

4. Verification

We verify our customers using electronic and document-based verification procedures and we use the procedures as set out in Annexure D to verify our customers.

We rely on the documentation-based safe harbour rules, to verify the identity of our customers if the client fails the electronic verification. We collect primary photographic identification documents and secondary identification documents (or certified copies of those documents) in accordance with Annexure D.

As we rely on the documentation-based safe harbour rules to verify the identities of our customers, where COVID-19 measures are preventing us from relying on original and/or certified copies of documents, we are still able to rely on the safe harbour rules by relying on copies of the documents, in accordance with risk-based systems and controls.

As we verify KYC information about a customer using the electronic safe harbor rules (which means we use reliable and independent electronic data), we complete the procedures set out in Annexure E for each electronic verification source.

As we verify the identity of our customers using reliable and independent documentation, without relying on the documentation-based safe harbour rules, we comply with the procedures set out in Annexure F.

5. KYC re-fresh procedure

Every 12 months from the date of the initial onboarding of the customer, we repeat the KYC checks on each customer (and their beneficial owners) to confirm whether there has been any change to the customer or to their business, that is:

- details of any changes to the nature of the business relationship of the customer;
- details of any changes in relation to the customer's control structure; and
- details of any changes to the beneficial ownership of the customer.

We conduct the customer re-fresh procedure at risk-based period, for example, re-fresh high-risk customer every 6 months, medium-risk every 12 months, and low-risk every 2 years.

Following the collection of the above information, if there are any changes as outlined above, we will:

- update the customer's details to reflect the new information collected;

  conduct a re-assessment of the customer's ML/TF risk level using Annexure C;

  in accordance with the ML/TF risk assessment, re-identify and re-verify the customer's identity using the appropriate identification and verification procedure in Annexure D in accordance with the customer type; and

- implement any appropriate ongoing customer due diligence procedures.

Where a customer cannot provide satisfactory evidence of identity

Where a customer does not possess, and is unable to obtain, the necessary information or evidence of identity, then in limited and exceptional cases, we may use alternative identity proofing processes, which are commensurate with our risk-based systems and controls.

In these limited and exceptional cases, the matter will be referred to the AML/CFT compliance officer, who may accept a self-attestation from the customer, if they are not aware that the self- attestation is incorrect or misleading. The AML/CFT compliance officer will also designate the customer as being high-risk and will implement the appropriate level of ongoing customer due diligence procedures which is commensurate with a high-risk customer.

6. PEPs and sanctions

6.1 PEP checks

We identify whether an individual is a PEP before we provide our services to the customer, or as soon as practicable after providing the designated service to the customer.

We check whether any individual customer, or beneficial owner of a non-individual customer identified as a foreign PEP, or an international organisation PEP, is included in the Consolidated List.

If the customer provides us with information that they have been employed by or connected with a New Zealand Government department or agency (domestic PEP), we look up the relevant department or agency in the Government Online Directory, and check whether the person is the head of the department or agency.

We subscribe to GBG and Comply Advantage which compares the customer's name and identification details to a range of databases, to identify whether the customer or beneficial owner is a PEP.

When selecting and monitoring the third-party service provider of sanctions and PEP checks, our AML/CTF compliance officer complies with the procedure outlined in Annexure E: Electronic Verification, and ensures that the procedures used by the third-party service provider:

- align with the PEP definition used in New Zealand; and
- identify when names will not be matched or when certain categories of PEPs are excluded; and
- identify when inconsistent spelling and/or transliterations of names may affect the results of the PEP checks.

We will not enter a business relationship with or provide our services to an individual or beneficial owner who is:

- a foreign PEP;
- an international organisation PEP (rated high-risk);
- a domestic PEP (rated high-risk); or
- an immediate family member or close associate of any of the above,

without obtaining the written approval of the AML/CFT compliance officer or Senior Management. Where Senior Management approval is required, the AML/CFT compliance officer ensures that senior management considers these issues in a timely manner. We also ensure that we establish their source of wealth and source of funds.

We have implemented risk-based systems for customers who are former PEPs or are the immediate family members or close associate of a former PEP. For more information, please refer to our PEP policy.

6.2 Sanctions

We subscribe to GBG and Comply Advantage which compares the customer's name and identification details to a range of databases, to identify whether the customer or beneficial owner is subject to sanctions.

6.3 Discrepancy

If we identify a discrepancy during the identification or verification or re-verification of KYC information about a customer, whether that customer is an individual or other type of entity, or about a beneficial owner of a customer, we will not provide services to the customer, and the AML/CFT compliance officer will be notified immediately. An example of a discrepancy may include that the identification provided by the customer appears to be forged, tampered with, cancelled, or stolen.

If a discrepancy arises while identifying and verifying a customer's identity, we will not provide any of the designated services to the customer until the discrepancy has been resolved.

Depending on the nature of the discrepancy, our AML/CFT compliance officer may undertake one or more of the following additional checks of the customer's identity, and decide about whether to commence or continue with the business relationship with the customer:

Requiring additional documentation which may include:

- citizenship certificate;
- birth certificate;
- change of name certificate;
- electronic verification identity check;
- proof of incorporation certificate; and/or
- other documents relevant to the situation.

If a discrepancy arises, as well as the additional measures outlined above, we will implement the Ongoing Customer Due Diligence process.

7. Ongoing Customer Due Diligence

We are obliged to monitor our customers and their **transactions on an ongoing basis** (ongoing customer due diligence, or OCDD).

OCDD helps us to:

- identify;
- mitigate; and
- manage,

any money laundering or terrorism financing risks that may arise from providing services to our customers, which arise at any stage **after the initial customer identification process has been completed**.

The difference between customer identification and OCDD is that customer identification should be undertaken prior to us providing a designated service and involves collecting and verifying initial KYC information.

7.1 What are the requirements of OCDD?

There are three mandatory components of OCDD:

1. *Collection and verification of additional customer identification information*

We have defined trigger points in our Program for collecting **additional** KYC information after the initial customer identification process is completed.

Some examples of trigger points include:

- if a customer or a beneficial owner is designated "high-risk", as set out in the customer risk assessment process above. This includes:
    - if a customer or beneficial owner is a PEP;
    - if a customer or beneficial owner becomes a PEP since they originally became a customer;
- if we enter into a transaction with a party physically present in a foreign country, or is a corporation incorporated in a foreign country;
- if we provide our services to a customer or a person associated with the transaction who is located in or connected to a high-risk jurisdiction;
- if a transaction for a significant amount occurs more than 50,000 NZD deposit per month
- if a customer makes a significant change to the way that their account has operated in the past for example, if the customer's account details move offshore to a high-risk jurisdiction, or there is a significant increase in the value or volume of transactions;
- if we have doubts regarding a customer's identity (such as the use of aliases and/or a variety of addresses);
- if a customer changes contact details and/or bank account details often;
- if one of the triggers for the transaction monitoring program has been flagged; or
- if a suspicious matter involving a customer has been reported to Financial Intelligence Unit (FIU).
- a customer favours anonymity or is reluctant to have a phone conversation with us;
- a customer requests a time-critical or urgent transaction without reasonable explanation;
- there are discrepancies in the identification information provided by the customer;
- a customer's occupation and income (source of funds) cannot be confirmed or is inconsistent with the customer's transaction profile;

- a customer is processing a level of transactions incompatible with their work status;
- a customer requests an undue level of secrecy during all interactions with us;
- a customer is subject to law enforcement action;
- an internet search brings up negative media results;
- a customer's provided name is different than the customer's payment method name;
- a customer's resident country is not New Zealand;
- a customer is listed on PEP & OFAC lists (country, names);
- a customer exceeds or asks to exceed their transaction limits;
- a customer tries to make a payment, using a card issued outside New Zealand;
- a customer is flagged as being on a Watchlist;
- there are discrepancies in the identification information provided by the customer;
- concerns are raised as a result of the customer's behaviour during the verification call;
- a customer starts acting out of character;
- a customer deposits funds into their account, and attempts to withdraw funds from their account without transacting;
- the source of funds is a bequest under a will;
- the customer enquires if we accept large cash deposits;
- the customer's predominant source of funds is from cash transactions;
- the average age and occupation check we have performed on the customer is inconsistent with the annual income and net worth provided by the customer;
- the customer's trading frequency and/or volume is greater than expected for the customer's annual income and net worth provided;
- the customer requests unusual/uneconomic investments;
- the customer asks for advice on how to evade tax;
- the customer has money or corporate entities based in tax havens;
- funds from several sources are consolidated into the customer's account;
- the members or trustees of an SMSF change several times over a short period of time;

The **additional** KYC information that we collect includes:

- the customer's and beneficial owner's source of wealth;
- the customer's and beneficial owner's source of funds;
- more details about the customer's occupation or business;
- clarification of the customer's ongoing relationship with us;
- undertake more detailed analysis of the customer's information and/or transaction history; and
- copies of the customer's most recent income tax returns, electronic pay slips, accountant certificates and bank statements

- Businesses and/or professional references from the customer's bank or professional advisers.

All additional KYC information collected in accordance with this procedure is dealt with in accordance with our record keeping obligations, set out in chapter 4 titled "Record Keeping" of this Program.

- documents showing source of wealth, such as:
    - income tax returns;
    - electronic pay slips;
    - latest bank statements;
- customer to provide proof of employment and income;
- if the source of a customer's funds or wealth cannot be ascertained, undertake more detailed analysis of the customer's information.

2. Transaction monitoring program

We have in place a transaction monitoring program to ensure that any discrepancies, anomalies and unusual or suspicious transactions are identified, and, if yes, the appropriate monitoring and supervision measures are implemented in relation to that customer.

The transaction monitoring program is run daily.

The transaction monitoring program highlights the transactions that might present an increased risk that ML/TF, tax evasion or fraudulent activities are taking place, and implements policies and procedures designed to manage and mitigate that increased risk.

Our transaction monitoring program includes the following procedures:

a) We monitor the transaction behavior of all customers, to identify whether any of the trigger points in the collection and verification of additional customer identification information section above are present. For example, additional monitoring may be implemented for all customers during their first 6 to 12 months of receiving your services or may only be triggered if the customer's transactions exceed a defined limit.

b) As part of our monitoring program, we also check whether any of the indicators of suspicious activity are present.

8. Suspicious Matter Reporting

8.1 What will we look for? Suspicious matter indicators

A suspicious matter usually arises during business dealings between us and the customer. In these situations, we will look out for information that may be related to:

- tax evasion; or
- criminal activity; or

- money laundering; or
- financing of terrorists.

As a rule, we will report any transaction that causes us or our employees to have a feeling of apprehension or mistrust about the transaction considering:

- its unusual nature or circumstances;
- the person or group that we are dealing with;
- all the other things that we know about that customer; and/or
- the behaviour (verbal or physical) of that person

Indicators of suspicious transactions are:

Customer profile

- the customer is a PEP;
- the customer starts transacting in amounts that differ from their usual transactions (e.g. a customer who usually transacts in amounts up to $1,000 starts to transact in amounts greater than $10,000 without reasonable explanation);
- the customer starts transacting at a higher frequency or amount than usual and there is no reasonable explanation;
- the customer is reluctant to use normal banking facilities;
- the customer frequently changes devices used to conduct transactions;
- the origin of the customer's wealth or source of funds cannot be easily verified;
- the customer is suspected of presenting false identification and verification information;
- information provided by the customer contradicts information gathered by us from other sources;
- doubts as to whether a customer is acting on their own behalf, or where it appears that the customer is acting on behalf of another person and the other person cannot be identified or is difficult to identify;
- the customer appears to be attempting to transact unexplained wealth, when compared with the KYC information we have collected;
- the customer exhibits unusual concern regarding government reporting requirements and this Program, including in relation to any of our other related policies and procedures;
- the customer is reluctant to provide information regarding their business activities, or the identification and/or business documents provided by the customer are vague or difficult to verify;
- upon request, the customer fails to indicate any legitimate source for their funds or wealth;
- the customer opens accounts in the name of family members or nominees;
- the customer is involved in unusually complex legal structures with no economic or logistical rationale;

- if we become aware that the customer has used false ID documents;
- if the customer or potential customer is unwilling to meet our ID requirements during the onboarding or customer application process;
- comments by the customer about tax evasion or other illegal activity;
- the customer is excessively concerned with privacy and confidentiality;
- the customer has businesses that operate in foreign jurisdictions, including high-risk jurisdictions, secrecy jurisdictions, or jurisdictions which have targeted financial sanctions and/or travel bans imposed by the United Nations Security Council;
- the customer has ID documents that originate from a high-risk or secrecy jurisdiction;
- the customer's background is unknown, or his/her reputation is suspicious;
- the customer is known to be aligned or loyal to a cause whose objects are themselves suspicious;
- the customer asks us to advise on or devise a radical change in the financial strategy, or exhibits a sudden and unexpected change in their pattern of trading activity;
- the customer insists on entering into financial commitments which appear to be beyond the customer's means;
- the customer, when migrating from one financial product or service to another, carries a different type and/or higher level of ML/TF risk;
- the customer has a history of changing financial services providers or using multiple financial services providers;
- the customer claims to be investing a gift or inheritance when this appears to be unsubstantiated;

Transaction behavior

- a customer performs (or instructs us to undertake) a transaction that does not appear to be driven by ordinary commercial considerations;
- a customer seems to be under serious financial stress, and normal rules of commerce appear to have been suspended;
- the customer starts acting out of character (for example, the customer makes unusual requests in relation to the movement of funds, or informs you of a new connection with a high-risk jurisdiction);
- funds from several sources are consolidated into the customer's account;
- where the customer requests deposit of funds/cash into our bank account;
- where the customer opens an account and requests correspondence is sent to an unrelated address;
- collateral is provided by third parties but the amount of funding does not appear to correspond to the financial profile of the customer;
- the customer has an inordinately large number of accounts for the type of business they are supposedly conducting;

- the customer has several or multiple complex accounts under one or more names and/or in more than one country, with regular inter-account transfers of aggregated funds not related to any legitimate business or commercial purpose;
- the customer opens a trading account, deposits a large sum of money followed by minimal or no trading;
- the customer requests regular, large transfers to overseas accounts;
- the customer withdraws large sums of cash from accounts, without providing a valid reason;
- the customer uses a personal account into which many different persons, perhaps in different places, are depositing cash;
- the customer seeks to designate a bank account in the name of a third party as the destination for financial income and investment returns;
- the customer directs transactions through an account that is suspected of being a shell company account;
- the customer is involved in high value transactions and requires rapid transfers across accounts in different countries and regions of the world;
- inconsistent pattern of denominations in currencies;
- large 'one-off' transactions, deposits or transfers, which relate to our services, but without a reasonable explanation;
- the customer is known to be involved with companies or accounts in "high-risk" countries, that is, any country known to be a tax haven, source or narcotics or other significant criminal activity or any country subject to trade sanctions;
- the beneficial owners or beneficiaries of the non-individual customers are resident in a "high-risk" country;
- there are gaps in know your customer (KYC) information;
- business activities of the customer are inconsistent with the customer's instructions or transaction history;
- activities of corporate customers, such as:
    - the use of the resources of a public company to further the private interests of the company's officers;
    - the payment of secret commissions;
    - payment of large management fees to entities associated with directors or management;
    - directors or management fraudulently acting against the interests of their company.

8.2 Reporting a Suspicious Matter

If at any time when dealing with a customer, we form a suspicion that an offence, tax evasion or other criminal activity may be taking place, we must lodge a report with FIU **within 3 business days** of forming the suspicion or **within 24 hours** of forming the suspicion, if our suspicion relates to the financing of terrorism.

This obligation relates to suspicious matters about any designated service that we provide, propose to provide or have been asked to provide by a customer or potential customer.

We have implemented the following procedure for reporting suspicious matters:

- All employees are required to report any potentially suspicious matters to the AML/CFT compliance officer as soon as they are aware of the issue.
- The AML/CFT compliance officer must promptly investigate, and, if they form the view that an SMR should be submitted, immediately notify the Compliance Committee or the Board.
- The AML/CTF compliance officer maintains a Suspicious Matter Register, which records each suspicious matter report which has been lodged with FIU.

Who is to be notified?

The AML/CFT compliance officer is the contact officer for submitting all suspicious matter reports.

All employees and officers of the Company will notify the AML/CFT compliance officer of their suspicions within **4 hours** of forming the suspicion.

We will **not** notify the customer who is demonstrating suspicious activity and will **not** disclose to anyone outside the business any information about the existence or contents of the report. To do so is an offence (the tipping-off prohibition).

We instruct our employees and agents to take care they do not do or say anything that may tip off the customer in this situation. This obligation is included in employee training.

We may, however, disclose suspicious matter information to the following people or entities, without breaching the tipping-off prohibition:

- to our lawyers, in order to obtain legal advice;
- to our external auditors, who are conducting a review of our AML/CFT Program;
- to other members of our corporate group located in New Zealand we deem it appropriate to inform the other members of the group of the risks involved in dealing with the particular customer;
- to comply with a requirement under Commonwealth, State or Territory law;
- to foreign members of our corporate group, who are regulated by one or more laws of a country that gives effect to some or all the FATF Recommendations, where we deem it appropriate to inform those members of the risks involved in dealing with the customer; or
- to a New Zealand government law enforcement body.

When providing suspicious matter information to foreign members of our corporate group, we ensure that the foreign related body corporate has given us a written undertaking in relation to receiving suspicious matter information from us, which:

- protects the confidentiality of the suspicious matter information;
- sets out strict controls on the use of the information;

- ensures that it will only be used for the purpose for which it is disclosed; and
- Confirms the foreign entity's understanding that the disclosure is made for the purpose of informing the foreign entity about the risks involved with dealing with the relevant customer.

We understand that we may breach any duty of confidentiality that we may owe to the customer when talking to FIU. The AML/CFT Act 2009 protect individuals and companies from any breaches of confidentiality in these situations. However, failure to report a suspicion may constitute an offence.

8.3 How to report suspicious activity reports (SARs)

The report must be completed online via goAML system and it will be completed by the AML/CFT Compliance Officer. The AML/CFT compliance officer is responsible for sending the SARs to FIU within the required timeframes.

Within 3 days of the suspicion being formed, we will do at least one of the following to assist FIU's investigation:

- complete customer identification, if this has not already been done;
- collect all relevant KYC information which relates to the customer; and
- verify the KYC information which relates to the customer.

If, because of the above procedures, the transaction monitoring program identifies a customer or transaction where a red flag has been triggered, we will implement the following controls:

i. collect and verify additional KYC information;
ii. seek the approval of the AML/CFT compliance officer as to whether to continue with a specific transaction and whether to continue the business relationship with the customer;
iii. obtain further information about the customer;
iv. obtain information about the source of wealth or funds the customer; and
v. undertake more detailed analysis of the customer's information and/or transaction history.

We will include other monitoring and supervisory strategies including but not limited to:

vi. imposing additional screening on the customer, so that all transactions over 100,000 AUD are reviewed by the AML officer.
vii. place a hold on the customer's account until the red flag has been investigated and an acceptable explanation for the behavior is ascertained;
viii. only allow the customer access to our services if each transaction is reviewed and signed off by the AML/CFT compliance officer.

The transaction controls referred to above will remain in place for a minimum of 6 months or at the discretion of the AML/CFT compliance officer and will only be removed with the approval of the AML/CFT compliance officer.

If a customer is the subject of the transaction monitoring program more than twice in a 12-month period, then the customer will be barred from receiving our services.

Additional KYC information below may also be collected.

- customers whose predominant source of funds are derived from cash or cash-equivalent;
- transactional activity that appears excessive for the customer, given their known source of funds;
- customers who change their personal details (e.g. email address) and subsequently change their funding source;
- we detect an unusual rise in the amount of transactions/activity in a client account;
- the customer makes large deposits and/or withdrawals (over $50,000 monthly);
- the customer requests to transfer money to sanctioned countries;
- the customer asks to transfer money to third parties;
- the customer asks us to facilitate irregular transactions that are outside of the norm for that customer;
- any unadvised transactions/activity by the customer.

3. Enhanced customer due diligence program

We understand that individual customers or beneficial owners which are current or former foreign PEPs or are immediate family members or close associates of current or former foreign PEPs, are automatically rated as high-risk.

We have an enhanced customer due diligence program in place to assess and collect further customer information in situations where we determine that:

a customer or beneficial owner is rated as high ML/TF risk (as determined according to the customer risk assessment procedure (set out in Annexure B);

- we are providing a service to an individual customer or a beneficial owner foreign PEP, or an immediate family member or a close associate of a foreign PEP (as this person is rated as high ML/TF risk;
- we are providing a service to an individual customer or a beneficial owner who is a former foreign PEP, or an immediate family member or a close associate of a person who is a former foreign PEP;
- we are providing a service to an individual customer or beneficial owner of a domestic or international organisation PEP, where that customer or beneficial owner has been rated as high ML/TF risk;
- a party to the transaction is physically located in a prescribed foreign jurisdiction;
- one of the grounds for reporting a suspicious transaction is present; or

- we enter or intend to enter a transaction, and a party to the transaction is physically present in, or is a company incorporated in, a prescribed foreign country.

If any of the above triggers occur, we will:

- seek further information from the customer or third-party sources to:
    - clarify/update the customer's information;
    - obtain further information about the customer; and/or
    - obtain information about the source of wealth or funds the customer;

  analyse the information that we have already collected and verified about the customer (including information about the beneficial owner, if applicable) – this may involve re-doing the procedure set out in Annexures B, C and D;

- determine which information needs to be clarified, updated or obtained about the customer or the nature of their business with us;
- consider whether additional transaction monitoring procedures should be implemented for this customer;
- obtain further KYC information or beneficial owner information (if applicable), including identifying the source of the customer's wealth and funds, using reasonable measures;
- clarify the nature of the customer's business relationship with us;
- verify or re-verify KYC, including beneficial owner information;
- undertake more detailed analysis of the customer's transactions in the past and in the future, including the purpose of the transactions, and the nature and level of transaction behavior (see our transactions monitoring program above);
- undertake more detailed analysis of the customer's information; and
- seek Senior Management approval for continuing a business relationship with the customer, whether to continue to provide a service to that customer, and whether a particular transaction should be processed.

If we suspect on reasonable grounds that the customer is not who they claim to be, within 14 days we will do at least one of:

1. collect any KYC information in respect of the customer; or
2. verify, from a reliable and independent source, KYC information that has been obtained in respect of the customer,

   to enable us to be reasonably satisfied that the customer is the person they claim to be.

If a suspicious matter arises, we will do one or more of the following within 14 days:

1. carry out the applicable identification procedure, unless we have already done so;
2. collect any KYC information in respect of the customer;
3. verify from a reliable and independent source the KYC information that has been obtained in respect of the customer, for the purpose of enabling us to be reasonably satisfied the customer is the person they claim to be.

Who does this requirement apply to?

OCDD obligations apply to all customers who receive a designated service from us.

Following the above extra identity verification procedures, if the AML/CFT compliance officer still suspects that the customer is not the person the customer is claiming to be, the AML/CFT compliance officer must then consider whether to lodge a suspicious activity report, as well as report the discrepancy to other relevant authorities (for example, FMA and NZ Police).

Re-verification

Where one or more of the customer's material details have changed, e.g. name, place of address, etc., we will update our KYC information by going through the processes set out in the attached Annexures B and C.

Documentation

We keep copies of the ID documentation on file for at least 7 years.

Annexure A: List of Jurisdictions – Risk Ratings

Before we provide designated services to a customer from a foreign jurisdiction, we will assess the jurisdictional risk associated with the foreign customer according to the table below:

Basel Institute on Governance: 2020 Public Basel AML Index Scores[i]	**FATF member country**[ii]	**Non-FATF country**	**UN Security Council and Australian Government sanctions list**[iii]	**FATF list of deficient jurisdictions**[iv]	**EU list of non-cooperative tax jurisdictions**[v]
6.5-9.0 (High risk)	Medium risk	High risk	High risk	High risk	High risk
4.0-6.49 (Medium risk)	Low risk	Medium risk	High risk	High risk	High risk
0.0-3.9 (Low risk)	Low risk	Low risk	High risk	High risk	High risk

If a country is subject to sanctions imposed by the Australian Government, (in **bold**), it is automatically rated as high-risk.

Country	Basel Index Score	ML/TF ranking (L, M, H)
A		
Afghanistan	8.16	H
Albania	5.72	H
Algeria	6.74	M
American Samoa	-	H
Angola	7.02	H
Anguilla	-	H
Antigua and Barbuda	4.95	M
Argentina	4.63	L
Armenia	4.63	M
Australia	3.75	L
Austria	4.42	L
Azerbaijan	5.24	M
B		
Bahrain	4.50	M
The Bahamas	6.46	M
Bangladesh	5.84	M
Barbados	5.82	H
Belgium	3.94	L
Benin	6.85	H
Bermuda	4.75	M
Bhutan	6.24	M
Bolivia	6.20	M
Bosnia – Herzegovina	5.63	M

Country	Basel Index Score	ML/TF ranking (L, M, H)
Botswana	4.87	H
Brazil	5.02	L
Bulgaria	3.12	L
Burkina Faso	6.77	H
C		
Cambodia	7.13	H
Canada	4.67	L
Cayman Islands	7.66	H
Cape Verde	6.49	H
Central African Republic	-	H
Chile	3.82	L
China	6.70	M
Colombia	4.64	M
Cook Islands	3.13	L
Costa Rica	4.74	M
Cote d'Ivoire	6.78	H
Crimea and Sebastopol	-	H
Croatia	3.95	L
Cuba	5.75	M
Cyprus	4.95	M
Czech Republic	4.28	M
D		
Democratic People's Republic of Korea (Nth Korea)	-	H

Country	Basel Index Score	ML/TF ranking (L, M, H)
Democratic Republic of the Congo	-	H
Denmark	3.46	L
Dominica	3.88	H
Dominican Republic	4.72	M
E		
Ecuador	4.89	M
Egypt	5.19	M
El Salvador	4.96	M
Eritrea	-	H
Estonia	2.36	L
Ethiopia	6.77	H
F		
Fiji	5.56	H
Finland	3.06	L
Former Federal Republic of Yugoslavia	-	H
France	3.92	L
G		
Gambia	5.29	M
Georgia	4.82	M
Germany	4.42	L
Ghana	4.88	M
Greece	3.67	L
Grenada	4.12	M

Country	Basel Index Score	ML/TF ranking (L, M, H)
Guam	-	H
Guatemala	5.12	M
Guinea-Bassau	-	H
Guyana	5.4	M
H		
Haiti	8.49	H
Honduras	5.52	M
Hong Kong Sar, China	5.20	L
Hungary	5.04	M
I		
Iceland	4.16	L
India	5.15	L
Indonesia	4.68	M
Iran	-	H
Iraq	-	H
Ireland	4.45	L
Israel	3.83	L
Italy	4.57	L
J		
Jamaica	5.77	H
Japan	4.99	L
Jordan	5.60	M
K		
Kazakhstan	5.08	M

Country	Basel Index Score	ML/TF ranking (L, M, H)
Kenya	7.18	H
Korea, South	4.61	L
Kyrgyzstan	6.09	M
L		
Laos	7.82	H
Latvia	4.61	M
Lebanon	5.33	H
Liberia	6.25	M
Libya	-	H
Lithuania	3.51	L
Luxembourg	4.74	L
M		
Madagascar	7.40	H
Macao SAR, China	5.93	M
Macedonia	3.89	L
Malaysia	5.47	L
Mali	7.37	H
Malta	5.45	H
Marshall Islands	5.57	M
Mauritania	8.13	H
Mauritius	5.32	H
Mexico	5.09	L
Moldova	4.98	M
Mongolia	6.09	M

Country	Basel Index Score	ML/TF ranking (L, M, H)
Montenegro	3.75	L
Morocco	5.32	H
Mozambique	7.71	H
Myanmar	7.83	H
N		
Namibia	-	H
Nepal	-	H
Netherlands	4.56	L
New Zealand	3.53	L
Nicaragua	6.75	H
Niger	-	H
Nigeria	6.89	H
Norway	3.35	L
O		
P		
Pakistan	6.00	H
Palau	6.17	H
Panama	6.00	H
Papua New Guinea	-	H
Paraguay	6.45	M
Peru	4.50	M
Philippines	5.76	H
Poland	4.36	M
Portugal	3.85	L

Country	Basel Index Score	ML/TF ranking (L, M, H)
Q		
Qatar	5.87	M
R		
Romania	4.79	M
Russian Federation	5.49	H
Rwanda	-	H
S		
Samoa	5.32	H
San Marino	3.42	L
Sao Tome & Principe	-	H
Saudi Arabia	5.12	M
Senegal	7.25	H
Serbia	5.47	M
Seychelles	5.29	H
Sierra Leone	7.00	H
Singapore	4.56	L
Slovakia	3.37	L
Slovenia	3.30	L
Solomon Islands	6.74	H
Somalia	-	H
South Africa	4.83	L
South Sudan	-	H
Spain	3.59	L
Sri Lanka	6.51	H

Country	Basel Index Score	ML/TF ranking (L, M, H)
St Lucia	5.21	M
St Vincent and the Grenadines	4.48	M
Sudan	-	H
Sweden	3.36	L
Switzerland	4.89	L
Syria	-	H
T		
Taiwan	4.39	M
Tajikistan	5.97	M
Tanzania	6.22	M
Thailand	6.15	M
Timor Leste	6.31	M
Trinidad and Tobago	4.85	H
Tunisia	5.20	M
Turkey	5.70	L
U		
Uganda	7.18	H
Ukraine	5.21	H
United Arab Emirates	5.91	M
United Kingdom	4.05	L
United States	4.60	L
Uruguay	3.98	L
US Virgin Islands	-	H
Uzbekistan	5.71	M

Country	Basel Index Score	ML/TF ranking (L, M, H)
V		
Vanuatu	5.33	H
Venezuela	6.56	H
Vietnam	7.04	H
W		
X		
Y		
Yemen	7.12	H
Former Federal Republic of Yugoslavia	-	H
Z		
Zambia	6.03	H
Zimbabwe	6.54	H

Annexure B: Customer Risk Assessment and KYC Process

Before we provide a designated service to the customer for the first time (even when we have provided services to the customer in the past), we categorise customers into either a low, medium, or high ML/TF risk category. That categorisation will determine what needs to be identified and verified. We undertake this procedure for each customer, using Annexure C.

As our AML/CFT Program is risk-based, if a customer is rated as being high-risk, we implement additional identification and verification procedures at onboarding, and additional Ongoing Customer Due Diligence procedures may also be triggered.

Step 1 – Customer risk assessment

The "Step 1" tab of Annexure C sets out the ML/TF risks faced by our business in relation to each of the following risk types:

- customer type;
- services/product type;
- method of delivery;
- source of wealth and funds;
- customer behaviour: nature and purpose of the reporting entity's relationship with customers;
- control structure of non-individual customers; and
- jurisdiction.

We have listed each of the risk indicators based on the risk types listed above in the "Step 1" tab and have allocated a risk between -1 and +5 or +50 for each risk, according to the following values:

Number	Risk level
-1	Moderate decrease in risk
0	No or negligible risk
1	Low risk
2	low/medium risk
3	Medium risk
4	medium/high risk
5	High risk
50	Automatically high risk

The values that we have allocated for the risks of each indicator are provided in Column D "Your Value" of the "Step 1" tab. In some instances, we have also provided comments in column E of the "Step 1" tab to justify why we have chosen values.

The risks and risk ratings flow through to the "CRA" tab of Annexure C.

We use the "CRA" tab to determine the risk rating of each customer at the commencement of our relationship with the customer. To assess the risk posed by each customer, we work through the list of risks that we have identified, and for each risk that is relevant to that customer, we type a "Y" or "X" in the grey shaded box to the left of the applicable risk.

The total sum of all the relevant risks is calculated and the customer is rated as low, medium, or high risk, according to their "score".

A customer will be rated as low, medium, or high risk as follows:

Score: 0-15: low risk
15-30: medium risk
Over 30: high risk

We may also refer to the "CRA" tab when performing ongoing customer due diligence and use it in the same manner to determine the customer's risk.

Step 2 – Identify the customer

Once we have categorised a customer as low, medium, or high ML/TF risk, we identify the customer in accordance with the fields set out in the relevant tabs, as set out in Annexure D. The level of detail we obtain will depend on the customer's risk rating.

Before we obtain personal information about the customer (for example, date of birth or address), we ensure that the customer has received our privacy statement that is publicly available on the company website https://www.thinkmarkets.com/nz/support/legal-and-regulation/privacy-policy/.

We then complete the relevant information in Annexure D appropriate to that type of customer:

- For an **individual, Individual Beneficial Owner** or **sole trader**, we identify and verify the customer in accordance with the procedure in the Individual tab.
- For a New Zealand **company**, we identify and verify the customer in accordance with the procedure in the NZ Company tab
- For a **foreign company**, we identify and verify the customer in accordance with the procedure in the Foreign Company tab
- For a **partnership**, we identify and verify the customer in accordance with the procedure in the Partnership tab
- For a **trust**, we identify and verify the customer in accordance with the procedure in the Trust tab
- For a **government body**, we identify and verify the customer in accordance with the procedure in the Govt Body tab
- For an **incorporated association**, we identify and verify the customer in accordance with the procedure in the incorporated association tab
- For an **unincorporated association**, we identify and verify the customer in accordance with the procedures in the unassociated association tab
- For a **registered co-operative**, we identify and verify the customer in accordance with the procedure in the registered co-operative tab

Forms are available from the AML/CFT compliance officer, and as part of this policy.

Step 3 – Verify the customer's identity

We then verify the details obtained in Step 2.

Option 1: The traditional method

We collect the documents from the customer and other sources as set out in the appropriate customer tab in Annexure D.

Option 2: The online verification method (electronic verification)

We verify the information collected about a customer, based on:

- reliable and independent documentation; or
- reliable and independent electronic data from at least two (2) separate data sources; or
- a combination of both above.

We have appointed GBG and Comply Advantage to undertake electronic verification on our behalf.

As we verify the identity of customers using reliable and independent electronic data, we ensure that the procedures outlined in Annexure E are complied with.

If the provider of online verification cannot verify the customer, we will use our processes as set out in Option 1 of this procedure.

AML/CFT compliance officer

The AML/CFT compliance officer ensures that the integrity of the online verification data is tested at least annually by using different authentication methods on a sample of customer files.

Errors

Any errors determined by us or by the provider of the electronic verification, must be considered at Compliance Committee/ Board meetings. If the Compliance Committee/Board or AML/CFT compliance officer forms the view that the errors are causing us to breach our obligations, we will revisit this procedure and the appointment of the current external online verification provider.

Step 4 – Where a customer cannot provide satisfactory evidence of identity

Where a customer does not possess, and is unable to obtain, the necessary information or evidence of identity, then in limited and exceptional cases, we may use alternative identity proofing processes, which are commensurate with our risk-based systems and controls.

In these limited and exceptional cases, the matter will be referred to the AML/CFT compliance officer, who may accept a self-attestation from the customer, if they are not aware that the self- attestation is incorrect or misleading.

The AML/CFT compliance officer will also designate the customer as being high-risk and will implement the appropriate level of ongoing customer due diligence procedures, which is commensurate with a high-risk customer.

Annexure C: Customer Risk Assessment Tool

Please refer to TM AML-CTF Annexure C V.1

Annexure D: KYC Customer Onboarding Tool

Please refer to TM AML-CTF Annexure D V.1

Annexure E: Electronic Verification Procedure

This process helps us to comply with our obligations in relation to electronic verification of customers and is a control to the electronic verification risk identified in our Risk Register.

Overview

If we verify the identity of customers using electronic data, the AML/CFT compliance officer ensures that the provider of online verification services provides us with details of the reliable and independent data sources it uses, and confirms that its verification processes:

- use accurate data (from at least 2 data sources);
- use secure data;
- have satisfactory processes in place to ensure data is up-to-date;
- are sufficiently comprehensive for our business type (by considering the range of persons included in the data and the period over which the data has been collected);
- include data from reliable and independent sources;
- clearly show which components of the data is maintained by a government body or pursuant to legislation; and
- allow for the electronic data to be additionally authenticated.

Verification

Where an individual customer or beneficial owner is rated as low or medium ML/TF risk, we comply with the electronic safe harbour provisions as follows:

Item no	Customer information to be verified	Number of separate data sources to be used for verification (minimum)
1	Name	2
2	**Either or both** Residential address Date of birth	2 2

Step 1: Details of the electronic verification provider

Name of the electronic verification provider

Name of company: GBG
Address: Level 4 / 360 Collins St, Melbourne, Victoria, Australia 3000
Email: contact@gbgplc.com
Tel: +61 (0) 385 951 500

Name of contact person at the electronic verification provider

Name: Amy Shurmer
Email: Amy.Shurmer@gbgplc.com
Tel: 0435 744 249

Step 2: Details of the electronic verification services

List of data sources relied on by the service provider

Item no	Name of data source
1	New Zealand Telephone
2	New Zealand Driving Licence
3	New Zealand Directors
4	New Zealand Property
5	New Zealand Vehicle
6	New Zealand DIA Birth
7	New Zealand DIA Citizen
8	New Zealand DIA Passport
9	New Zealand MVR
10	New Zealand Credit

11	Watch lists: Consolidated List (DFAT); Office of Foreign Assets Control (US Treasury); Politically Exposed Persons (CIA World Leaders publications)

Step 3: Assessment of the data source

List of pre-defined tolerance levels for matches and errors

Assessment of the data source

The purpose of this section is so that we can determine whether the electronic data that the service provider relies upon is reliable and independent.

For each of the data sources listed, we provide an assessment (i.e. a rating out of 10, where 10 is the highest and 1 is the lowest).

We use the following table to complete the assessment for each data source:

Name of data source

Attributes of data source	**Assessment rating (out of 10)**
Accuracy of the data	
Security of the data	
How comprehensive is the data	
Whether the data been verified from a reliable and independent source	
Whether the data is maintained: • by a government body; or • pursuant to legislation	
Whether the data can be additionally authenticated	
Rating (out of 60):	

For each data source, the rating of each attribute contributes to an overall rating whereby:

Rating score	**Assessment of data sources**
Between 1 and 30	Not reliable and independent

Between 30 and 60	Reliable and independent

Step 4: Additional information to be collected for high-risk customers

If a customer is rated as high ML/TF risk, we conduct the additional KYC checks set out in the customer type tabs in Annexure C [or D], as well as the ongoing and enhanced customer due diligence procedures set out in Part A

In addition to following the procedure for a low or medium risk customer, the service provider will:

- Consult one additional data source to verify the customer's identity, which has been assessed as being reliable and independent.

Step 5: Attach documents to customer's file

We attach a copy of the report from the service provider used to verify the customer, together with the client's application in Management Portal.

Annexure F: Documentation Verification Procedure

This process helps us to comply with our obligations in relation to document-based verification of customers who are assessed as posing a low or medium ML/TF risk, where we do not rely on the documentation-based safe harbour rules.

The procedures set out in this Annexure were created in accordance with our ML/TF Risk Assessment and have been designed to manage and mitigate the risk that our business could be used for ML/TF.

If a customer is assessed as posing a high ML/TF risk, then in addition to the procedures set out below, the customer is identified, and their identity verified using the enhanced customer due diligence procedure set out in this policy.

Overview

If we verify the identity of customers using documents, but without relying on the documentation-based safe harbour rules, we have implemented appropriate risk-based systems and controls (as set out in this Annexure) for us to determine:

- For individual customers:
    - what reliable and independent documentation we will collect to verify the individual's name and date of birth and/or residential address, or to verify any other KYC information;
    - when we will rely on a copy of a document;
    - how we determine whether a document has been forged, tampered with, cancelled or stolen;
    - whether we use any authentication services, and if yes, details of the services we use;
    - any other measures we use to confirm that the KYC information about an individual is correct, including by independently initiating contact with the person.
- For non-individual customers:
    - what reliable and independent documentation we will collect to verify a customer's identity;
    - whether a document is sufficiently contemporaneous to be used for verification;
    - when we will rely on a copy of a document;
    - how we determine whether a document has been forged, tampered with, cancelled or stolen;
    - whether we use any authentication services, and if yes, details of the services we use;
    - any other measures we use to confirm that the KYC information about a customer is correct, including by independently initiating contact with the customer.

A. Verification of individual customers

No.	Requirement	Our procedure
1	What reliable and independent documents do we use for verification?	• Valid passport; or • driver's licence; and • current bank statement/rate notice/utilities bill issued within the last 6 months
2	In what circumstances do we rely on copies of verification documents?	We accept the following copies of verification documents: • a digital photo of the individual customer holding their driver's licence; or • a scanned copy of the document.
3	How do we determine whether a document has been forged, tampered with, cancelled, or stolen?	We provide our employees with detailed training to enable them to identify whether the document is forged or has been tampered with. Our operations manual also sets out examples of documents which have been forged or tampered with. Employees are directed to seek the guidance of the AML/CFT compliance officer.
4	What other measures do we use to confirm whether the KYC information about a customer is correct?	Calling the client with the phone number listed on the application or sending an email to the email address provided to confirm the details in the verification documents.

B. Verification of non-individual customers

No.	Requirement	Our procedure
1	What reliable and independent documents do we use for verification?	• Company: current FMA company search/ minutes of Board meeting • Trust: NZBN search/ extract of the trust deed • Partnership: extract of partnership deed/ minutes of partnership meeting
2	Is the document sufficiently contemporaneous?	• Company search: must be dated within 1 month of the verification date • Minutes of meetings: must be within 3 months of the verification date

No.	Requirement	Our procedure
3	In what circumstances do we rely on copies of verification documents?	We accept scanned copies of verification documents.
4	How do we determine whether a document has been forged, tampered with, cancelled, or stolen?	We provide our employees with detailed training to enable them to identify whether the document is forged or has been tampered with. Our operations manual also sets out examples of documents which have been forged or tampered with. Employees are directed to seek the guidance of the AML/CFT compliance officer.
5	What other measures do we use to confirm whether the KYC information about a customer is correct?	Calling the client with the phone number listed on the application or sending an email to the email address provided to confirm the details in the verification documents.

If a customer is rated as high ML/TF risk, we conduct the additional KYC checks set out in the customer type tabs in Annexure D, as well as the ongoing and enhanced customer due diligence procedures set out in this policy.

All KYC documents are subject to the following principles:

Principle 1 – clear documents:
Documents may be in colour or black and white copy. No partial images blurred or low quality/resolution. Clients may cover transactions for bank statements and/or credit card numbers for credit cards but it must be clear to see whether the document is genuine.

Principle 2 – original documents
Documents should be in good condition and showing no signs of alteration (manually or electronically).

Principle 3 – "current" documents
Documents must be issued within 6 months unless it was issued less frequently, e.g. passports, ID card etc.

Principle 4 – sufficient information
ID documents must show full name, date of birth, issue, and expiry date. Address documents must show issue date and name of issuer. Address documents received in the post are preferable

Principle 5 – online generated documents
All online printouts and screenshot must show the account name and address of the applicant. We will only accept online generated documents of utility bills and bank statements.

Principle 6 – coherence
Information must be logically consistent across all documents and application (same name, same date of birth, same address, same photograph, and same signature). Any mismatches must be clarified with the applicant before submission for approval. Indication of forgery should not be ignored and must be notified to Compliance, e.g.: a passport and a national ID card showing a different date of birth.

Principle 7 – translation of documents
The translation must be carried out using the standard template. Documents must be translated in full (all information displayed) specifying all the required information. e.g.: date of issue, name of body/company issuing the document etc.

N.B. All Principles and procedures in this document are non-negotiable. It is your obligation to collect all required documents and ensure all documents submitted can satisfy the Principles. In the event of documents not meeting the requirements above, the approach will be decided on a case-by-case basis and it will probably result in a delay in the application process.

Proof of ID

Proof of ID must be signed and show the client's name and date of birth as entered in the application. The document must be current however some countries issue ID documents without an expiry date.

For certain ID documents, we will require a copy of the front and the back as some of the information will be contained on the back of the document.

If the name on the ID document does not match the name in the application, the applicant will have to submit a new application entering the correct information.

It is possible to approve an application if the name mismatch is due to a shortened version of the same name or missing middle names. We can accept the documents below:

1. Current signed passport.
2. Government issued National Identity Card.
3. A valid government ID, such as a Driver's License or State ID.

Proof of Address

Documents used as proof of address must have an issue date and show the applicant's name, address. If the address on the document does not match the application, the applicant will have to provide a new POA document with the correct address. We can accept the documents below:

1. Current recent utility bill (dated within the last 6 months) that clearly states the applicant's name and address.
2. Local Authority tax bill (valid for the current year).
3. Current full driving license (if it has not been used as evidence of personal identity).
4. A statement or confirmation note produced by another regulated financial sector firm indicating that an account/investment/insurance relationship exists, and which contains the customer's address.
5. Tenancy agreement.
6. Bank Letter.
7. Attested Notarised Letter of residency.

There are certain cases when applicant might not have address document under his/her name due to documents being under name of parents or spouse. We can accept a document under different name if we verify marriage certificate or ID of a parent.

All New Zeland residents/citizens applying for an account in New Zeland (residence address shows Australia) must pass the suitability test.

Client Suitability Test – Below steps need to be followed to approve NZ resident client.

- Option 1 – Complete an online Test with a Pass mark of 70%
- Option 2 – Provide a trading statement detailing trading experience with another ASIC broker.
- Option 3 – Provide evidence of completion of trading course with FMA registered training provider.

We can accept New Zealand issued Driver's License or Passport on its own given that:

- The photo is clear
- Document looks genuine
- Comply Advantage performed and no positive match were found
- Address, Name and Date of Birth are verified electronically through Trulioo.

Application IP address:

As part of a risk assessment, ThinkMarkets tracks the IP address from which the application is received. If the applicant from a particular country has applied from a different location, the KYC specialist must confirm such mismatch via email and the risk-based approach should apply while confirming the mismatch.

Trulioo

If the client was not electronically verified, and the client only provided a copy of his passport or driver's licence, Trulioo may be use as another system to verify the client and if the client was Trulioo verified, we may run Comply Advantage for PEP and sanctions check and approve the client's application.

Corporate Applications

The level of due diligence to be applied to a corporate will vary depending on whether it is a private, regulated, or public listed firm.

Once the Corporate Application form is completed, signed, and returned, the On-boarding team will begin the due diligence process. The information provided by the corporate applicant will determine the steps required to verify the company.

Please note if any of the directors or shareholders are US citizens or residents, they must be referred to compliance for further verification.

It is vital to identify the Ultimate Beneficial Owner (UBO) of our non-individual customers.

Assessment:

Like all other business and Money Laundering/ Terrorism Financing (ML/TF) risks, beneficial owner risks change over time. It is important that you regularly review your beneficial owner risk assessment and ensure processes are up-to-date and reflect current risk factors.

Determination:

A beneficial owner of a non-individual customer is an individual that controls the customer, or either directly or indirectly owns 25% or more of the customer.

The beneficial owner's (or beneficial owners') interest in the non-individual customer will often be indirect. This means they do not directly own 25% or more of the customer themselves, but they own an interest in another entity, which in turn owns an interest in the non-individual customer.

There can be several links in the chain of ownership that need to be traced through to determine the beneficial owner(s).

Collection of information:

You must collect at minimum the full name of each beneficial owner, as well as either their date of birth or their full residential address. To verify the beneficial owner's (or beneficial owners') identity, you need to use reliable and independent documentation or reliable and

independent electronic data that demonstrates the identity information you collected about the beneficial owner is correct.
The beneficial owner(s) of non-individual customers may change over time, so you need to regularly update beneficial owner information throughout the life of relationships with non-individual customers.

Record keeping:

You must keep records of the beneficial owner identification process that you undertake. Importantly, you should ensure you keep records to demonstrate you have traced through each link in a non-individual customer's chain of ownership, until you have identified all individuals who meet the definition of UBO.

UBOs will be identified when assessing non-individual documents. All non-individual clients must provide register of directors and shareholders. If one of the shareholders is a legal entity, you would have to verify UBOs as well. This procedure will keep going until we get to individuals in charge.

Once UBO is identified his identity will be verified according to his geographical risk classification. All UBOs must provide government issued ID and proof of address as minimum. Information collected from UBO will be verified through GBG or Comply Advantage.

If identity of UBO cannot be established, you need to use a disclosure certificate. Disclosure certificates may only be used for verification purposes as a last resort when other verification methods are unsuccessful. Please keep record of attempts to verify the identity before using Disclosure certificates.

If identity of UBO cannot be established, you cannot on-board the customer.

Every non-individual account must provide LEI. It is a mandatory requirement and account cannot be opened without providing an LEI.

What is an LEI?

LEIs are required for the purpose of identifying counterparties that are legal entities (including those in trusts) in ASIC transaction reports.

LEIs are a unique 20-digit alphanumeric code which offers standard credibility and aids in managing the identity of an eligible entity in any business transaction.

According to the Global LEI Foundation (GLEIF) over 1,150,000 LEIs have been issued.

How to obtain an LEI

LEIs are issued by Local Operating Units (LOU) accredited by the GLEIF. A list of all Local Operating Units can be found on the GLEIF website.

LEI must be checked by KYC member and verification needs to be done on official GLEIF website https://www.gleif.org/en/lei/search and ensure it is issued, active, and belong to the same company's name and country.

Confirmation of LEI needs to be saved and uploaded under Compliance documents to client profile.

Self-managed Superfunds (SMSF)

We can only open an account with a self-managed superfund if the trustee is a qualified investor. Eligibility requirements:

- Investing $500,000 or more;
- Net assets of $2.5m* or above; or
- Gross Income of at least $250,000 per annum for two consecutive financial years*

*Accountant's certificate issued within the last two years required.

***This is additional information for SMSF, but we do not currently onboard CFD SMSF until further notice.

Glossary

- **"the Act"** means the Anti-Money Laundering and Countering Financing of Terrorism *Act 2009*
- **"AML"** means anti-money laundering.
- **"beneficial owner"** means an individual who ultimately **owns** or **controls** an entity.
- **"certified copy"** means a document that has been certified as a true copy of an original by either a person authorised to witness statutory declarations, a legal practitioner, an officer or authorised representative of an Australian Financial Services Licensee or an Australian Credit Licensee, or a person in a foreign country who is authorised by law in that jurisdiction to administer oaths or affirmations or to authenticate documents.
- **"close associate"** means a person who has joint beneficial ownership of a legal entity with that person, or sole beneficial ownership of an entity that exists for the benefit of that person.
- **"the Company"** means TF Global Markets (Aust) Pty Ltd and is referred to in this Program as we, us, our, it, or the Company.
- **"control"** means control by means of an arrangement or agreement which results in the person exercising control of an entity through the capacity to determine decisions about financial and operating policies.
- **"CFT"** means Countering Financing of Terrorism.
- **"disclosure certificate"** is a certificate which is signed by or on behalf of a customer (being a domestic company, a foreign company, a trust, an incorporated or unincorporated organisation or a registered co-operative) by an officer of the customer, which contains various information, including, at a minimum, the full name and residential address of each beneficial owner of the customer.
- **"document-based safe harbour rules"** means the documentation-based safe harbour procedure, which may be relied upon where the customer's ML/TF risk is medium or low, and involves the following verification process:
    - verify the customer's name and either their residential address and/or date of birth from:
        - an original or certified copy of a primary photographic identification document; or
    - verify the customer's name and either their residential address and/or date of birth from both:
        - an original or certified copy of a primary non-photographic identification document; and
        - an original or certified copy of a secondary identification document; and
    - verify that the document produced has not expired (other than a Commonwealth passport, which can be relied upon for verification if it expired within the preceding 2 years).
- **"domestic PEP**" means a politically exposed person of a New Zealand government body, but does **not** include persons holding positions at local government or municipal levels.

"electronic safe harbour rules" means the electronic safe harbour procedure, which sets out the procedure for determining whether the electronic data used to verify the identity of a customer is reliable and independent. See Annexure E for the procedure.

"FATF Recommendations" means the internationally endorsed global standards against money laundering and terrorist financing, created by the Financial Action Task Force (FATF).

- "**FIU***" is the* Financial Intelligence Unit (FIU) sits within the Financial Crime Group framework and is mandated to assist with the detection and investigation of money laundering, terrorism financing and other offences.
- **"foreign PEP**" means a politically exposed person of a government body of a foreign country, including persons holding positions at local government or municipal levels.
- **"Inland Revenue"** is the one collecting the revenuw that government needs to fund its programmes.
- **"international organisation"** means an organisation established by formal political agreement by two or more countries with the status of an international treaty and recognised in the laws of the countries which are members of the organisation.
- **"international organisation PEP"** means a politically exposed person of an international organisation.
- **"KYC"** means know your customer.
- **"ML"** means money laundering.
- **"ML/TF risk"** means the risk that that we may reasonably face that, in providing the designated services, we are involved in or facilitate money laundering or terrorism financing.
- **"money laundering"** is the processing of criminal profits to disguise their illegal origin.
- **"OCDD"** means ongoing customer due diligence.
- **"owns"** means ownership of 25% or more of an entity.
- **"PEP" or "politically exposed person"** means an individual entrusted with a prominent public function (for example, Heads of State, government, senior politicians, or senior executives of state-owned companies, but not usually a middle rank or junior official), and includes:
    - a person who is an immediate family member of that person, including spouse, de facto partner, child, child's spouse or partner or parent; and
    - a **close associate** of that person.
- **"primary non-photographic identification document"** includes:
    - a birth certificate or birth extract issued by the government;
    - a citizenship certificate issued by the government;
    - a citizenship certificate issued by a foreign government that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator;
    - if the individual or beneficial owner holds dual citizenship, obtain citizenship certificates or other citizenship documents issued by both governments;

- a birth certificate issued by a foreign government, the United Nations or an agency of the United Nations that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator;
- a pensioner concession card, a health care card or a senior's health care card.

- **"primary photographic identification document"** includes:
  - a licence or permit issued, or equivalent authority of a foreign country, for the purpose of driving a vehicle that contains a photograph of the person in whose name the document is issued;
  - a passport issued by the government;
  - a passport or a similar document issued for the purpose of international travel, that:
    - contains a photograph and the signature, or any unique identifier of the person in whose name the document is issued;
    - is issued by a foreign government, the United Nations, or an agency of the United Nations; and
    - if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator;
  - a card issued under a law of a State or Territory for the purpose of proving the person's age, which contains a photograph of the person in whose name the document is issued;
  - a national identity card issued for the purpose of identification, that:
    - contains a photograph and the signature, or any unique identifier of the person in whose name the document is issued;
    - is issued by a foreign government, the United Nations or an agency of the United Nations;
    - if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator.
- **"reasonable measures"** means appropriate measures which are commensurate with our assessment of the ML/TF risk.
- **"secondary identification document"** includes:
  - a notice that:
    - was issued to an individual by the government within the preceding twelve months;
    - contains the name of the individual and his or her residential address; and
    - records the provision of financial benefits to the individual under a law of the country (as the case may be);
  - a notice that:

        - was issued to an individual by the Inland Revenue within the preceding twelve months;
        - contains the name of the individual and his or her residential address; and
        - records a debt payable to or by the individual by or to (respectively) the government under government law relating to taxation;
    - a notice that:
        - was issued to an individual by a local government body or utilities provider within the preceding three months;
        - contains the name of the individual and his or her residential address; and
        - records the provision of services by that local government body or utilities provider to that address or to that person;
    - in relation to a person under the age of 18, a notice that:
        - was issued to a person by a school principal within the preceding three months;
        - contains the name of the person and his or her residential address; and
        - records the period that the person attended the school.
- **"Senior Management"** specifically refers to the Board, the Compliance Committee, and the AML/CTF compliance officer.
- **"terrorism financing"** refers to the financing of terrorist acts, and also of terrorists and terrorist organisations.
- **"TF"** means terrorism financing.
- **"threshold transaction"** means any physical cash transaction where the total amount of the transaction is at least NZ $10,000.

Endnotes

[i] The Basel AML Ranking is amended annually and can be found at https://index.baselgovernance.org/ranking.
[ii] The AML/CTF status of jurisdictions are checked via: http://www.fatf-gafi.org/countries.
[iii] The UNSC and Australian Government Sanctions can be found at: https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes
[iv] The FATF List of deficient jurisdictions is found at: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html
[v] The EU List of non-cooperative taxation jurisdictions is found at: https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/