BCR
Bridge The Difference

AML Policy

4 July 2019

BCR
BVI Company No.1975046
License No. SIBA/L/19/1122

BCR Co Pty Ltd (BCR)

Standard Anti-Money Laundering and Counter-Terrorism Financing Program

Part A (General)

1. Requirement for Program

As a reporting entity under the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 ('Code'), BCR is required under Section 11 of the Code to adopt an Anti-Money Laundering and Counter-Terrorism Financing Program ('Program') structured in compliance with rules issued from time to time by the Financial Services Commission ('Commission'). BCR has adopted this Code under Regulation 3 of the Anti-Money Laundering Regulations, 2008, to satisfy these requirements.

The Nominated Contact Officer for BCR is Mr. Victor Ringor.

2. Purpose of Program

This Program is divided into two parts: Part A (general) and Part B (customer identification).

1. Part A is designed to identify, mitigate and manage the risk that BCR may reasonably face in providing designated services that might (whether inadvertently or otherwise) involve or facilitate:

   (a) money laundering; or
   (b) financing of terrorism.

2. Part B sets out the applicable customer identification procedures for customers of BCR.

3. Board Approval of Program

This Program has been approved by the Board of BCR.

It is an offence under the AML/CTF Code not to comply with this Program once adopted by the Board.

4. Application of Program

This Program applies to all businesses conducted by BCR involved in the provision of a designated service, including any functions carried out by a third party on its behalf.

5. Outline of regulatory requirements

The purpose of the AML/CTF Code is to thwart money laundering ('ML') and the financing of terrorism ('TF') within BVI's jurisdiction and to assist international efforts in confronting organised crime and terrorism. The Code attempts to achieve these goals by requiring providers of transactional, or designated, services

to verify the identities of their customers and to report suspicious activity to the Financial Investigation Agency. Part A of this Program seeks to gather information to enable BCR to:

(1) understand the nature and purpose of the business relationship with customer its types, including as appropriate, the collection of relevant information relevant to that understanding; and
(2) understand the control structure of non-individual customers;
(3) identify significant changes in ML/TF risk for the purposes of Part A and Part B of this Program
(4) recognize such changes in ML/TF risk for the purposes of the requirements of Part A and Part B of this Program
(5) assess the ML/TF risk posed by:
a. all new designated services prior to introducing them to the market;
b. all new methods of designated service delivery prior to adopting them;
c. all new or developing technologies used for the provisions of a designated service prior to adopting them; and
d. changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers.

This program implements the obligations imposed on BCR by the AML/CTF Code. In summary, these obligations are:

Table 1: Summary of AML/CTF obligations imposed

Obligation	Time Requirement	Paragraph Reference
Collect identification documents and verify identities of customers (investors).	Before, or at, the time that an interest is issued to the customer. Whilst the designated services are rated as Medium Risk, the collection and verification of identities may occur within 5 days after the services have been provided.	Part A – Section 7.1 Part B
Conduct further inquiries where a suspicion is held that an advised identity by customer seeking a Medium Risk designated service is false.	Initiate with 14 days of forming a suspicion of a false identity.	Part A – Section 7.1.2 Part B
Carry out ongoing due diligence of customers to identify suspect matters.		Part A – Section 7.2.1 Part A – Section 7.2.2
Report suspicious activity to the Financial Investigation Agency.	Within 3 days of forming a suspicion relating to ML (this is in addition to the 14	Part A – Section 7.4

	days to conduct further enquiries in relation to a customer's identity per 2). Within 24 hours of forming a suspicion relating to TF.	
Conduct due diligence of employees.		Part A – Section 8.5

5.1 Money laundering

Money laundering ('ML') is dealing in money or property which are the proceeds of crime, or which may otherwise be used to commit a crime. This includes proceeds of crimes committed in each State and Territory, Federal and international jurisdictions. Dealing, in this context, includes:

1. the receipt, possession, concealment or disposal of money or other property;
2. the importation of money or other property into, or exportation of money or other property from, BVI; and
3. engaging in a banking transaction relating to money or other property.

5.2 Financing of Terrorism

The financing of terrorism ('TF') is the intentional receipt of funds from, or the provision of funds to, a terrorist organisation. A terrorist organisation is an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act.

5.3 Designated Services

5.3.1 Services Provided by BCR

BCR is a reporting entity under the AML/CTF Code because we provide the following designated services:

Table 2: Designated Services provided by BCR

Sec. Ref	Designated Service
T.1, 35	issuing or selling a security or derivative to a person, where: (a) the issue or sale is in the course of carrying on a business of issuing or selling securities or derivatives; and (b) in the case of an issue of a security or derivative—the issue does not consist of the issue by a company of either of the following: (i) a security of the company (other than

	an interest in a managed investment scheme); or (ii) an option to acquire a security of the company (other than an option to acquire an interest in a managed investment scheme); and (c) in the case of an issue of a security or derivative—the issue does not consist of the issue by a government body of a security of the government body or of an option to acquire a security of the government body; and (d) in the case of an issue of a security or derivative—the issue is not an exempt financial market operator issue; and (e) such other conditions (if any) as are set out in the AML/CTF Codes are satisfied.
T.1, 54	In the capacity of holder of an FSC financial services licensee, making arrangements for a person to receive a designated service.

5.3.2 Issuing or selling securities on a Prescribed Financial Market

For clarity, under of the AML/CTF Codes, issuing or selling of securities (including units in a managed investments scheme by way of a product disclosure statement, rights issue or a distribution reinvestment plan) on a Prescribed Financial Market are declared not to be designated services.

5.4 Requirement to verify identities of investors/agents

It is an offence to provide a designated service to a new investor without verifying their identity per the procedures set out in Part B of this Program.

6. Risk Assessment of designated services

Differing customer identification and verification standards apply according to whether the provided designated services are low or higher risk. Further, the Commission requires BCR, in determining what is an appropriate risk-based procedure for inclusion in Part B of this Program, to have regard to money laundering and terrorism financing risk relevant to the provision of its designated services.

BCR has adopted the following risk assessment procedures, which are modelled on the criteria set out in the Financial Action Task Force ('FATF'), *Guidance On The Risk-Based Approach To Combating Money Laundering And Terrorist Financing, High Level*

Principles and Procedures. The FATF guide proposes six assessment dimensions. These dimensions are broadly consistent with the Commission Guidance and the considerations set out, which are:

1. customer types, including:
    a. beneficial owners of customers, and
    b. any politically exposed persons;
2. its customers' sources of funds and wealth;
3. the nature and purpose of the business relationship with its customers, including, as appropriate, the collection of information relevant to that consideration;
4. the control structure of its non-individual customers; the types of designated services provided;
5. methods of delivery of the designated services; and
6. the foreign jurisdictions with which it deals.

This risk assessment has been applied to each designated service provided by BCR. A designated service is only considered to be medium risk if all responses to the listed criteria are rated as medium risk.

Designated Services: Issuing interests in registered managed investments schemes

Holding an FSC Licence and making arrangements for persons to receive designated services

(1) Investor types, including any politically exposed persons

This is an assessment of the risk of dealing with particular customers who may have a propensity to finance terrorist activities or to launder money.

Table 3: Risk assessment checklist of customer types, including PEPs

Number	Criteria	Medium Risk?
1.	No suspicion has been formed that that a material proportion of the investors have a history of suspicious transactions, such as: Significant and unexplained geographic distance between the institution and the location of the investors; Frequent and unexplained movement of accounts to different institutions; and Frequent and unexplained movement of funds between institutions in various geographic locations?	Yes

2.	In general, it is relatively easy to identify the owner of the financial products in which BCR has issued interests?	Yes
3.	Beneficial owners of corporate investors are not difficult to identify and/or verify?	Yes
4.	There are no known charities or not for profit organizations who have invested into the financial products who are not subject to either Government monitoring, independent Boards or governance, or annual audit?	Yes
5.	No accounts are known to be held in the name of a lawyer, accountant or other professional for the benefit of another person?	Yes
6.	Investors are not known, or suspected, to be a Politically Exposed Persons?	Yes

(2) Types of designated services provided

This is an assessment of the potential risks presented by products and services offered by BCR.

Table 4: Risk assessment checklist of product types and services

Number	Criteria	Medium Risk?
1.	No suspicion has been formed that that a material proportion of the investors have a history of suspicious transactions, such as: Significant and unexplained geographic distance between the institution and the location of the investors; Frequent and unexplained movement of accounts to different institutions; and	Yes

	Frequent and unexplained movement of funds between institutions in various geographic locations?	
2.	In general, it is relatively easy to identify the owner of the financial products in which BCR has issued interests?	Yes
3.	Beneficial owners of corporate investors are not difficult to identify and/or verify?	Yes
4.	There are no known charities or not for profit organizations who have invested into the financial products who are not subject to either Government monitoring, independent Boards or governance, or annual audit?	Yes
5.	No accounts are known to be held in the name of a lawyer, accountant or other professional for the benefit of another person?	Yes
6.	Investors are not known, or suspected, to be a Politically Exposed Persons?	Yes

(3) Methods of delivery of the designated services

This is an assessment of the potential risks presented by the manner in which the designated services are provided to investors.

Table 5: Risk assessment checklist of service delivery issues

Number	Criteria	Medium Risk?
1.	The services may only be provided on a submitted written application signed by the investor?	Yes
2.	An investor has no or little control over the investment decisions of BCR in the investments of the financial product?	Yes
3.	Payments of either capital or income out of the financial product are only paid directly by cheque to the investor or	Yes

	are otherwise paid by EFT to an account held in the name of the investor with an ADI or equivalent bank established in an FATF member country?	

(4) National jurisdictions in which the services are provided

This is an assessment of the risk of financing terrorist activities or money laundering by providing designated services in a particular national jurisdiction.

Table 6: Risk assessment checklist of jurisdictional exposure

Number	Criteria	Medium Risk?
4.	Is the customer a citizen of, and their account therefore based in, a FATF member country ('Source Country')? Current FATF member countries include: 1. Argentina 2. Australia 3. Austria 4. Belgium 5. Brazil 6. Canada 7. China 8. Denmark 9. European Commission 10. Finland 11. France 12. Germany 13. Greece 14. Gulf Co-operation Council 15. Hong Kong, China 16. Iceland 17. India 18. Ireland 19. Italy 20. Japan 21. Kingdom of the Netherlands 22. Luxembourg 23. Mexico 24. New Zealand 25. Norway	Yes

	26. Portugal 27. Republic of Korea 28. Russian Federation 29. Singapore 30. South Africa 31. Spain 32. Sweden 33. Switzerland 34. Turkey 35. United Kingdom 36. United States	
5.	Is the Source Country generally considered to be free from corruption or from overtly funding or supporting terrorist activities?	Yes

Risk Assessment: Medium

Based on the above assessment, Part B of this Program has adopted the Medium Risk investor identification and verification procedures allowed in the Commission Codes.

Under the AML/CTF Code is permissible to verify the identities of investors after the Medium Risk designated services have been provided to them.

The risk assessment above will be reviewed each year when then independent review of Part A of this program is undertaken, or when new services or distribution arrangements are entered into, in order to:

(1) identify significant changes in ML/TF risk for the purposes of Part A and Part B of this program;
(2) recognize such changes in ML/TF risk for the purposes of the requirements of Part A and Part B of this program; and
(3) assess the ML/TF risk posed by:
    (a) all new designated services prior to introducing them to the market;
    (b) all new methods of designated service delivery prior to adopting them; and
    (c) all new or developing technologies used for the provision of a designated service prior to adopting them.

7. AML/CTF Obligations

The obligations of the AML-CTF Code which apply to BCR are summarized in Table 1. This section expands on these obligations and summarizes the controls implemented to address them.

7.1 Initial Client Identification and Verification

Before a financial service may be provide to a customer, personal identification documents for that person must be obtained and that person's identity then objectively verified.

The documents required for identification and verification vary depending on whether the customer is a natural personal, corporation, foreign national, partnership or the like. The specific documentary requirements and verification procedures for each type of customer are set out in Part B of this Program.

Usually, it is anticipated that each customer will provide the required documents, and their identities will be verified, before they are issued an interest in a scheme or fund, or before they are provided with investment advisory services. However, because the designated services provided by BCR are assessed as Medium Risk, it may be possible to collect the documents and verify identities after the issue of the interests or after advice has been provided. It is expected that the discretion to defer collecting identification documents and verify customers' identities will only occur in circumstances where the AML/CTF Compliance Officer has been consulted before post service verification proceeds.

Clients will not be able to redeem any interests in a scheme operated by BCR until their identification documents have been provided and their identities verified.

7.1.1 Suspicion of false identity

Where a suspicion is formed that a person whose identity had been verified under the Medium Risk procedures is not who they claim to be or that they may be involved in suspicious transactions (see Section 7.2.2) then it will be necessary, within 14 days of forming the suspicion, to conduct further inquiries to verify the true identity of that person.

Any further inquiries undertaken must be done so in a manner that would not alert the person to the suspicion or to a report having been made to the Commission on the suspicion. It is a criminal offence to 'tip' a person to such a suspicion or a report being lodged on the basis of such a suspicion.

As examples, suspicions may be aroused where:

- Correspondence to the person are returned as undeliverable;
- The person does not provide a Tax File Number after a reasonable number of requests have been made for them to do so;
- Correspondence from the individual contains inconsistent information from that obtained when the application was first processed (different name spelling, date of birth, address details);
- The customer does not appear to recognize their name when contacted by telephone;
- In the case of natural persons, the customer provides office or post office addresses for correspondence instead of a fixed residential address;
- Another person attempts to communicate on matters concerning a customer's account under an actual or implied authority.

If, after further investigation, it is determined that the person has provided a false identity or that are reasonable grounds for suspecting that their identity is false, then it will be necessary to lodge a Suspicious Activity Report with the Financial Activity Agency.

The AML/CTF Compliance Officer is responsible for lodging such activity with Financial Investigation Agency.

7.2. Ongoing Client Due Diligence (KYC)

It is necessary to conduct ongoing customer due diligence to attempt to identity, mitigate and manage any ML or TF activities. This process is different from that in section 7.1 because it is concerned with the ongoing relationship with customers after they have invested or have established a service contract with BCR.

Ongoing customer due diligence involves two actions:

- Ensuring that the persons to whom the services are being provided are who they say they are; and
- Monitoring transactions to identify any unusual cash flows that may result from or be preparatory to ML or TF activities.

Know Your Customer ('KYC') information is broader than customer identity records obtained before providing a designated service to a customer. It will be necessary, within limits, to collect additional KYC information to either prove the identity of a customer or to determine whether or not they may be involved in a matter that should be reported to the Financial Investigation Agency.

For the different types of customer, KYC information may encompass:

(1) For individuals:
(a) the customer's full name
(b) the customer's residential address
(c) the customer's date of birth
(d) the full business name (if any) under which the customer carries on his or her business
(e) the full address of the customer's principal place of business (if any) or the customer's residential address
(f) any business number issued to the customer
(g) the nature of the customer's business with the reporting entity – including
(i) the purpose of specific transactions; or
(ii) the expected nature and level of transaction behavior;
(h) the income or assets available to the customer;
(i) the customer's source of funds including the origin of funds;
(j) the customer's financial position;
(k) the beneficial ownership of the funds used by the customer with respect to the designated services; and
(l) the beneficiaries of the transactions being facilitated by the reporting entity on behalf of the customer including the destination.

(2) For companies:

In the case of a domestic company:

(a) the full name of the company as registered
(b) the full address of the company's registered office
(c) the full address of the company's principal place of business (if any)
(d) the business number issued to the company;
(e) whether the company is registered as a proprietary company or a public company;
(f) if the company is registered as a proprietary company, the name of each director of the company;
(g) in the case of a registered foreign company:
(i) the full name of the company as registered
(ii) the full address of the company's registered office;
(ii) the full address of the company's principal place of business (if any) or the full name and address of the company's local agent in the BVI (if any);
(iii) the business number issued to the company;
(iv) the country in which the company was formed, incorporated or registered;
(v) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a proprietary or private company or some other type of company; and
(vi) if the company is registered as a private company by the relevant foreign registration body – the name of each director of the company;
(h) in the case of an unregistered foreign company:
(i) the full name of the company;
(ii) the country in which the company was formed, incorporated or registered;
(iii) whether the company is registered by the relevant foreign registration body and if so:
(A) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;
(B) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and
(C) whether it is registered as a proprietary or private company or some other type of company by the relevant foreign registration body;
(iv) if the company is registered as a private company by the relevant foreign registration body – the name of each director of the company, and
(iv) if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation;

(3) For trustees:

(a) the full name of the trust;
(b) the full business name (if any) of the trustee in respect of the trust;
(c) the type of the trust;
(d) the country in which the trust was established;
(e) the full name of the settlor of the trust, unless:
(i) the material asset contribution to the trust by the settlor at the time the trust is established is less than $10,000; or
(ii) the settlor is deceased; or
(iii) the trust is verified using the simplified trustee verification procedure
(f) if any of the trustees is an individual – in respect of any of those individuals, the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals;
(g) if any of the trustees is a company – in respect of any those companies, the information required to be collected from a company under the reporting entity's customer identification program in respect of companies;
(h) the full name and address of any trustee in respect of the trust;
(i) the full name of any beneficiary in respect of the trust;
(j) if the terms of the trust identify the beneficiaries by reference to membership of a class – details of the class; and
(k) a certified copy or certified extract of the trust deed.

(4) For partners:

(a) the full name of the partnership;
(b) the full business name (if any) of the partnership as registered under any State or Territory business names legislation;
(c) the country in which the partnership was established;
(d) in respect of one of the partners - the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals;
(e) the full name and residential address of each partner in the partnership except where the regulated status of the partnership is confirmed through reference to the current membership directory of the relevant professional association;
(f) a partnership agreement, certified copy or certified extract of the partnership agreement.

(5) For incorporated associations:

(a) the full name of the association;
(b) the full address of the association's principal place of administration or registered office (if any) or the residential address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer;
(c) any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association;

(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association;
(e) the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;
(f) the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association;
(g) information provided by the BVI or overseas body responsible for the incorporation of the association;
(h) in respect of any member – the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals.

(6) For unincorporated associations:
(a) the full name of the association;
(b) the full address of the association's principal place of administration (if any);
(c) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association;
(d) in respect of any member – the information required to be collected from an individual under the reporting entity's customer identification program in respect of individuals;
(e) a certified copy or certified extract of the rules of the association;
(f) the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;
(g) the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association; and

(7) For registered co-operatives:

(a) the full name of the co-operative;
(b) the full address of the co-operative's registered office or principal place of operations (if any) or the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer;
(c) any unique identifying number issued to the co-operative upon its registration by the relevant registration body;
(d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative;
(e) a certified copy or certified extract of the rules of the co-operative.

(8) For government bodies:

(a) the full name of the government body;
(b) the full address of the government body's principal place of operations;
(c) whether the government body is an entity or emanation, or established under Legislation of the BVI or a foreign country and the name of that State, Territory or country;

(d) information about the ownership or control of a government body that is an entity or emanation or established under legislation of a foreign country; and
(e) the name of any legislation under which the government body was established.

7.2.1 Monitoring customer identities

Monitoring customer identities will be a responsive process.

Where a customer's identity is suspected to be false, further inquiries will be made to correctly identify that person. Any further inquiries undertaken must be done so in a manner that would not alert the person to the suspicion or to a report having been made to the Commission on the suspicion. It is a criminal offence to 'tip' a person to such a suspicion or a report being lodged on such a suspicion.
Indicators that a customer's identity should be examined more closely include:

1. a change in a customer's signature from an initial application held on file
2. a request by a customer to change the source bank account from which EFTs may be accepted
3. a request by a customer to change the target bank account into which withdrawals from an investment service are to be paid
4. a request by a customer to accept transaction orders from another person authorised by the customer, or
5. noticeable changes in account management by the customer (e.g., high activity or unusual sized transactions).

7.2.2 Monitoring transactions

All transactions will be monitored in an attempt to identify suspicious transactions. The AML/CTF Code describes a suspicious transaction as including any activity related to a transaction that may be:

1. relevant to an investigation of, or prosecution of a person for, an evasion, or an attempted evasion, of a taxation law
2. relevant to an investigation of, or prosecution of a person for, an evasion, or an attempted evasion, of a law of a State or Territory that deals with taxation
3. relevant to investigation of, or prosecution of a person for, an offence against a law of a State or Territory
5. of assistance in the enforcement of a law of a State or Territory; or
6. which may be preparatory to the commission of an offence in the financing of terrorism or money laundering.

To provide guidance, the following transactions may be considered suspicious:

- investments made by cheque issued by a foreign registered bank (unless the customer has previously been identified as a foreign national within the jurisdiction of the domiciled bank);
- requests for withdrawal cheques to be made to cash;

- requests for withdrawal cheques to be paid to third parties;
- cash transactions; or
- investments made from unknown persons into a customer's account.

7.2.3 Enhanced Customer Due Diligence

Enhanced customer due diligence will be undertaken where:

(a) it determines that the ML/TF risk is high; or
(b) the customer is or has a beneficial owner who is, a foreign politically exposed person; or
(c) a suspicion has arisen in relation to the identity of the customer or customer's agent, or where the customer may be involved in a suspect transaction; or
(d) the customer is physically present in, or incorporated in, a prescribed foreign country.

Where enhanced customer due diligence is undertaken, BCR may:

(1) seek additional information from the customer or from third party sources in order to:
(a) clarify or update KYC information already collected from the customer;
(b) obtain any further KYC information, including, where appropriate, taking reasonable measures to identify:
(i) the source of the customer's wealth;
(ii) the source of the customer's funds; and
(iii) the ultimate beneficial ownership of the customer (if a non-individual);
(c) clarify the nature of the customer's ongoing business with the reporting entity.
(2) Undertake a more detailed analysis of the customer 's KYC information, including, where appropriate, taking reasonable measures to identify:
(a) the source of the customer's and each beneficial owner's wealth;
(b) the source of the customer's and each beneficial owner's funds.
(3) verify or re-verify KYC information in accordance with the customer identification program;
(4) verify or re-verify beneficial owner information in accordance the beneficial owner identification requirements in section 10.8 of Part B of this Program;
(5) undertake more detailed analysis and monitoring of the customer 's transactions – both past and future, including, but not limited to:
(a) the purpose or nature of specific transactions; or
(b) the expected nature and level of transaction behavior, including future transactions;
(6) seek senior management approval for:
(a) continuing with a business relationship with a customer; and
(b) whether the designated service should continue to be provided to the customer.
(7) consider whether a transaction or particular transactions should be processed.

Note: if the customer is, or has a beneficial owner that is, a politically exposed person, in addition to any other appropriate measures, BCR will carry out the measures in 7.2.3(2) and (6) above.

7.3. Suspicious Activity Reports

A suspicious activity report must be lodged with the Financial Investigation Agency by the AML/CTF Compliance Officer.

All potential suspicious activity must be presented to the AML/CTF Compliance Officer who will consult with the Chairman of the Risk Management Committee make the final determination on whether a report should be lodged.

Suspicious activity reports may be required at the following process points where:

Number	Process Point	Paragraph	Suspicion
1.	Potential Client inquiry about service	-	The potential customer may have provided a false identity.
2.			The transaction may relate to a criminal or tax avoidance matter.
3.			The transaction may be preparatory to ML.
4.			The transaction may be preparatory to TF.
5.	Initial Client Identification	7.1.2	The customer may have provided a false identity.
6.	------ " ------	7.1.1	The customer is listed on the Consolidated List.
7.	------ " ------	7.2.2	The transaction may relate to a criminal or tax avoidance matter.
8.	------ " ------	7.2.2	The transaction may be preparatory to ML.
9.	------ " ------	7.2.2	The transaction may be preparatory to TF.
10.	Ongoing Client Identification	7.2.1	The customer may have provided a false identity.
11.	------ " ------	7.2.1	The customer is listed on the Consolidated List.

12.	Reviewing Transactions	7.2.2	The transaction may relate to a criminal or tax avoidance matter.
13.	------ " ------	7.2.2	The transaction may be preparatory to ML.
14.	------ " ------	7.2.2	The transaction may be preparatory to TF.

A Suspicious Activity Report must be lodged with Financial Investigation Agency within 3 days of forming a suspicion in the case of matters that are not related to TF. As discussed above, these 3 days occur after the 14 days allowed to collect identification documents and to verify the identity of a suspicious customer who has been provided the designated service prior to the commencement of the Code. Suspicious Activity Reports concerning TF matters must be lodged within 24 hours of forming the suspicion.

The relevant customer must not be advised that a suspicious activity report has or will be lodged with Financial Investigation Agency. It is an offence under the Code to tip off a customer about a suspicious activity report.

7.4 Acquisitions of reporting entities

If BCR intends to acquire all or part of a designated service business from another reporting entity it must first determine:

(a) the ML/TF risk it faces in providing a designated service to the customers it will receive from the acquired business; and
(b) that it has in place appropriate risk-based systems and controls to identify, manage and mitigate the ML/TF risk it faces in providing the designated service to the customers it will receive from the acquired business; and
(c) based on the assessed ML/TF risk and its risk-based systems and controls, it is reasonable for it to either:
(i) rely upon the applicable customer identification procedures of the selling reporting entity as an appropriate means to identify and verify the identification of a transferring customer; or
(ii) treat a transferring customer who was a pre-commencement customer of the selling reporting entity as if the customer were a pre-commencement customer of BCR.

If BCR determines that:

(a) a suspicious activity report should be made in relation to a customer it received from the acquired business, or
(b) the selling reporting entity had not carried out the applicable customer identification procedures when it was required to do so; or

(c) a significant increase has occurred in the level of ML/TF risk as assessed under this AML/CTF program in relation to the provision of a designated service by BCR to the customers it has received from the acquired business, then within 14 days of the determination, BCR for the purpose of enabling reporting entity two to be reasonably satisfied that the customer is the person that he or she claims to be, must:
(1) carry out the applicable customer identification procedure, unless BCR has previously carried out that procedure or a comparable procedure; or
(2) collect any KYC information in respect of a customer; or
(3) verify, from a reliable and independent source, KYC information that has been obtained in respect of the customer, as is appropriate to the ML/TF risk relevant to the provision of the designated service by BCR.

8. Operational Elements of Program

8.1 AML/CTF Compliance Officer

BCR will appoint an AML/CTF Compliance Officer. This Officer may be either an employee or a consultant, and may also possess other responsibilities in addition to managing this Program.

BCR has determined to appoint Mr. Victor Ringor, a Responsible Manager, as its AML/CTF Compliance Officer.

The AML/CTF Compliance Officer will be responsible for:

1. updating this Program when required to encompass new or changed designated services, or to incorporate new requirements under law or by Commission Codes;
2. conducting reviews to ensure that the Program remains appropriate for the needs of BCR;
3. implementing a due diligence procedure to ensure that that the identity and verification records are current, accurate and securely stored;
4. perform testing to ensure that the procedures set out in Part B are implemented and followed by staff or service providers;
5. reporting suspicious activity to Financial Investigation Agency;
6. reporting on the effectiveness of this Program to the Board on a regular basis.
7. ensure that staff at all levels are aware of their responsibilities in relation to AML/CTF risk management.
8. assessing the money laundering and terrorism financing risk posed by:
    a. all new designated services prior to introducing them to the market;
    b. all new methods of designated service delivery prior to adopting them; and
    c. all new or developing technologies used for the provision of a designated service prior to adopting them.

In particular, the AML/CTF Compliance Officer will be responsible for ensuring that the following matters are identified and reported to the Board:

1. significant changes in money laundering and terrorism financing risk for the purposes of the Part A and Part B programs;
2. recognizing such changes in money laundering and terrorism financing risk for the purposes of the requirements of its Part A and Part B programs; and
3. assessing the money laundering and terrorism financing risk posed by:
    (a) all new designated services prior to introducing them to the market;
    (b) all new methods of designated service delivery prior to adopting them; and
    (c) all new or developing technologies used for the provision of a designated service prior to adopting them.

8.2 Money Laundering Reporting Officer (MLRO)

BCR will appoint an MLRO Officer. This Officer may be either an employee or a consultant, and may also possess other responsibilities in addition to managing this Program.

BCR has determined to appoint Mr. Victor Ringor, a Responsible Manager, as its MLRO Officer.

The MLRO Officer will be responsible for:

1. Receiving and considering reports from employees of activities and transactions giving rise to knowledge or suspicion of money laundering or terrorist financing;
2. Making onward reports to Financial Investigation Agency, where appropriate;
3. Acting as the key liaison point with the Financial Investigation Agency, the IRD/ITA, and other law enforcement agencies;
4. Maintaining a formal Register of all suspicious activity reports, the determinations made, any subsequent reports made to Financial Investigation Agency and the IRD/ITA, and any further correspondence sent or received.

8.3 Integration with the Business Risk Management Framework

BCR maintains a Business Risk Management Framework based on AS/NZS 4360:2004: Risk management. This framework encompasses both legal/regulatory and business operational risks. The framework documents all material risks held by the business, the agreed mitigating controls, their residual risks ratings (based on a standardized Consequence & Likelihood assessment), the person responsible for effecting the controls and the frequencies of the controls implementations.

All material risks and the agreed mitigating controls will be incorporated into this Framework. Consequently, the AML/CTF Compliance Officer will be responsible for reviewing the scope of the risks identified, assessing the residual risk ratings, monitoring performance and reporting on the effectiveness of the framework to the Board.

In particular, the framework will require a regular risk assessment of the designated services provided by BCR based on the criteria set out above.

In modifying the framework to address money laundering and terrorism financing ('ML/TF') risks consideration will be given to the specific risks set out in the Code. These specific risks include:

(a) failure to include all mandatory legislative components;
(b) failure to gain board and/or executive approval of the AML/CTF program;
(c) insufficient or inappropriate employee due diligence;
(d) frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s);
(e) changes in business functions which are not reflected in the AML/CTF program (for example, the introduction of a new product or distribution channel);
(f) failure to consider feedback from the Commission (for example, advice regarding an emerging ML/TF risk);
(g) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML/CTF program;
(h) legislation incorrectly interpreted and applied in relation to a customer identification procedure;
(i) customer identification and monitoring systems, policies and procedures that fail to:
    (i) prompt, if appropriate, for further identification and/or verification when the ML/TF risk posed by a customer increases;
    (ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;
    (iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
    (iv) take appropriate action where the identification document provided is neither an original nor a certified copy;
    (v) recognize foreign identification documentation issued by a high-risk jurisdiction;
    (vi) record comprehensive details of identification documents, for example, the date of issue;
    (vii) consult appropriate resources in order to identify high-risk customers;
    (viii) identify when an expired or old identification document (for example, a driver's licence) has been used;
    (ix) collect any other name(s) by which the customer is known; or
    (x) be subject to regular review;
(j) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs;
(k) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
    (i) customer identification policies, procedures and systems; or
    (ii) identifying potential ML/TF risks; and
(l) acceptance of documentation that may not be readily verifiable.

8.4 Control self-assessment procedures

The AML/CTF Compliance Officer will design and implement controls for effecting the AML/CTF Code. Operational staff will assist in this process.

The agreed controls will then be incorporated into the Compliance & Risk Management System maintained by BCR. In addition, the controls and hence controls self- assessment questionnaires/certificates will be incorporated into this process.

BCR recognises that the AML/CTF Code permits the inclusion of such controls into the Compliance Plans of its registered managed investments schemes. BCR has determined not to incorporate these controls into these statutory documents.

8.5 AML/CTF risk awareness training program

The AML/CTF risk awareness training program must be designed so that BCR gives its employees appropriate training at appropriate intervals, having regard to money laundering and terrorism financing risk it may reasonably face.

The AML/CTF training program must enable employees to understand:

1. the obligations of the reporting entity under the AML/CTF Code;
2. the consequences of non-compliance with the AML/CTF Code;
3. the type of money laundering and terrorism financing risk that the reporting entity might face and the potential consequences of such risk; and
4. those processes and procedures provided for by the BCR's AML/CTF program that are relevant to the work carried out by the employee.

Accordingly, the AML/CTF Compliance Officer will design a training program to address the above elements. This training program will be:

1. Provided to all staff and Directors on approval of this Program by the Board;
2. On appointment of all new employees and contractors; and
3. Where deemed necessary to enhance the awareness of Directors, staff and employees.

8.6 Employee due diligence program

BCR is required to establish an employee due diligence program. This program must:

- put in place appropriate risk-based systems and controls for BCR to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of a money laundering or financing of terrorism offence in connection with the provision of a designated service.

- include appropriate risk-based systems and controls for the reporting entity to determine whether to, and in what manner to, re-screen an employee where the employee is transferred or promoted and may be in a position to facilitate the commission of a money laundering or financing of terrorism offence in connection with the provision of a designated service.

- establish and maintain a system for the reporting entity to manage any employee who fails, without reasonable excuse, to comply with any system, control or procedure established in accordance with Part A or Part B.

Consequently, all prospective employees and contractors providing material services to BCR who may be in a position to facilitate the commission of money laundering or a financing of terrorism offence in connection with the provision of a designated service will be subject to a screening process. This process will involve, depending on the position held, a combination of:

1. Obtaining a Federal Police check to identify any previous charges or convictions;
2. Obtaining a Credit Reference check;
3. Interviewing at least 2 referees; and
4. Reviewing databases to identify if the persons have been banned or suspended from providing a financial service.

In addition to the above, all employees will be required to sign a statement stating that they have been provided with AML/CTF risk awareness training, are aware of the requirements, and have not and will not engage in any conduct that may result in breach of a provision.

Further, any employee who fails, without reasonable excuse, to comply with any system, control or procedure established in accordance with Part A or Part B of this program will be reported to the Board. Actions that may be taken to address such a situation include:

1. Counselling the employee;
2. Changing their positional duties;
3. Reducing their annual performance increment;
4. Formal performance management, including mandatory attendance of training programs;
5. Suspension of duties; and
6. Dismissal.

The particular action that will be taken will be determined based on:

1. The level of conscious disregard;
2. The level of the individual's responsibilities;
3. The risk to investors and BCR; and
4. Any other history of non-compliance or inappropriate behavior exhibited by the individual.

8.7 Independent review

Part A must be subject to regular independent review. Reviews must be conducted once per calendar year. The review may be carried out by either an internal or external party. The review must be conducted by a person who was not involved in the preparation, approval, implementation or oversight of the program and who has sufficient experience with the AML/CTF legislation and preferably has a compliance, accounting or legal background.

The independent reviewer will be provided with a scoping statement confirming that the purpose of the review should be to:

1. assess the effectiveness of the Part A program having regard to the money laundering and terrorism financing risk of the reporting entity;
2. assess whether the Part A program complies with the Code;
3. assess whether the Part A program has been effectively implemented; and
4. assess whether the reporting entity has complied with its Part A program.

The result of the review, including any report prepared, will be provided by the person who conducted the review to the Risk Management Committee and the Board of BCR.

8.8 Financial Investigation Agency feedback

All feedback provided by Financial Investigation Agency will be provided to the AML/CTF Compliance Officer in the first instance who will consider how to respond to the feedback.

All material Financial Investigation Agency feedback will be presented to the Board by the AML/CTF Compliance
Officer.

[End of Part A]

BCR Co Pty Ltd (BCR)

Standard Anti-Money Laundering and Counter-Terrorism Financing Program

Part B (Customer Identification)

1. Part B integral to Program

This is Part B of the Program adopted by the BCR. It is integral to, and must be read in conjunction with, Part A of the Program.

2. Purpose of Part B

This Part sets out the applicable customer identification procedures for customers of BCR.

3. Approval and modification of Part B

This Part was adopted by the Board of BCR when it approved the Program.

4. Summary of Customer Identification procedures

Part A provides an assessment of the designated services provided by BCR as Medium Risk. This document therefore reflects the customer identification and verification procedures for Medium Risk Designated services in the AML/CTF Codes.

These processes include:

1. Disclosing to investors their obligation to provide personal information and evidence which we will use to verify their identities.
2. Having a procedure for verifying identities based on the provided evidence.
3. Recording the evidence provided and the verification of identities.
4. Considering whether there is a suspicion that a proposed investor is not who they claim to be.
5. Reporting suspect activity to the Financial Investigation Agency within the required time frames.

5. Customers to whom the procedures will be applied

The requirement to verify the identities of investors applies to all customers of BCR.

6. Use of agents

It may be preferable to use agents to collect and verify the identities of customers through an agent. Such agents include Administrators (who process application forms, maintain the scheme registry, and may maintain the accounts of the scheme) and financial planners (who may arrange for investors to be issued interests in a scheme operated by BCR.

Agents also include reporting entities within a designated business group.

In appointing an agent, BCR recognises that it may not abrogate its responsibility under the AML/CTF Code to ensure that the identities of its customers are verified.

All agency appointments must be made in writing and BCR must determine that it is appropriate to rely upon the applicable customer identification procedure carried out by the agent. The terms of all agency appointments must:

1. Declare that the relationship between the BCR and the service provider is that of principal and agent for the purposes of collecting identification materials and verifying the identities of potential investors in the schemes offered by BCR.
2. That the agent will either:
    (a) provide copies of records made by the agent in accordance with the AML/CTF Code in respect of each customer; or
    (b) is otherwise bound to provide BCR with access to the records made by the agent in accordance with the Code.
3. Provide an indemnity for any consequential damages that may arise from the agent failing to obtain records, verify the identities, and make an appropriate record or from failing to meet privacy requirements in the handling of personal information provided by a customer.

7. Disclosure in Product Disclosure Statements and IMAs

All offer documents issued by BCR must provide information on the requirements for all new investors to disclose information and provide requested documentation to disclose their identities.

The application forms for all offer documents must make provision for the collection of the information set out below.

Whilst the designated services provided by BCR are considered to be Medium Risk, interests in any scheme or service offered will be issued on receipt of a completed application form and cleared application monies.

The identities of investors will be made prior to the issue of interests in a scheme or before a designated service is provided to them. Where an interest has been issued, but the investor's identity not verified, no payments of distributions, income or withdrawal requests will be honored. All income will be accrued to the investor's account until their identities may be verified. The potential to withhold payments must be set out in the relevant offer document.

Further, where a notice has been given by BCR to a customer to provide information that is likely to assist in complying with Part A of the program, and the customer does not provide that information, then BCR may refuse to provide or in continuing to provide the designated service to that customer. The potential to cease the provision of a designated service must be set out in the relevant offer document.

A suspicious activity report will be lodged with Financial Investigation Agency where an investor chooses not to or cannot or does not provide adequate documentation to permit their identity to be verified.

8. Privacy Requirements

All documentation and information provided by customers for the purposes of verifying their identities are considered to be personal information. This information is subject to the Privacy restrictions.

The collection of this information is a permitted matter under British Common Law. However, it is necessary to disclose to customers the source of the requirement for BCR to collect this information, to provide access to records of personal information held by BCR on that individual, to not use that information for any other purpose other than disclosed at the time of collection, not to pass that information onto any party, and to destroy that information once it is no longer needed.

9. Record keeping

The AML/CTF Code imposes a number of record-keeping obligations on reporting entities, including:

- Designated services provided
- Customer transactions
- Applicable customer identification procedures
- Electronic funds transfer instructions
- AML/CTF programs

A record must be made of each designated service provide to every customer. These records must be retained for at least 7 years after record was made.

All documents, or copies of all documents, provided by a customer to either BCR or its authorised agents for identification purposes must be retained for at least 7 years. Records of customer identification procedures are kept for the life of the customer relationship and an additional seven years after the reporting entity ceases to provide any designated services to the customer. This means that if a reporting entity has provided two designated services to a customer, the seven-year retention period would not begin until both designated services had ceased to be provided (rather than commencing separately as each designated service ends).

In addition, all records maintained by BCR or its authorised agents used to record the verification of a person's identity must be retained for at least 7 years.

All AML/CTF programs adopted by BCR must also be retained for at least 7 years commencing from the date that the adoption ceased to be in force.

10. Customer identification requirements – summary

Disclosure certificates

BCR may request that a customer provide a disclosure certificate if:

(a) it has determined that the information cannot otherwise be reasonably obtained or verified;
(b) the information to be provided or verified is reasonably required under this AML/CTF program;
(c) the relevant procedures and requirements in this AML/CTF program have been applied but BCR has been unable to obtain or verify the information

The Disclosure Certificate must be signed or otherwise authenticated by a director, company secretary, appointed AML/CTF Compliance Officer or trustee of the customer (if appointed) or an equivalent officer of the customer (such as a Compliance Officer).

The Disclosure Certificate may be made as a letter, using the term 'Disclosure Certificate' in the title header.

BCR will only accept investment applications made by way of:

1. cheque paid from an account held with a recognized local bank
2. EFT from an account held with a recognized local bank, or
3. EFT from an internationally recognized bank or pay service, or
4. a bank cheque payable by a recognized local bank.

Under no circumstances will BCR accept investments made as cash or in specie transfers from regulated or unregulated persons.

The following sets out the information or documentary evidence to be provided by all customers, the verifications that are to be performed on that evidence, and the records that are to be retained.

10.1 Natural Persons

10.1.1 Individuals

A. Identification information - individuals

(1) the customer's full name;
(2) the customer's date of birth; and
(3) the customer's residential address.

B. Verification of information - individuals

The following information must be verified for each individual from customer provided identity documents (see paragraph C. Identity documents – individuals):
(1) the customer's full name; and
(2) either:
(a) the customer's date of birth; or
(b) the customer's residential address.

C. Identity documents - individuals

Acceptable identity documents are listed in the Know-Your-Client (KYC) Evidence Verification Form. The usual acceptable identity documents are:

(1) an original or certified copy of a primary photographic identification document; or

(2) both:

(i) an original or certified copy of a primary non-photographic identification document; and

(ii) an original or certified copy of a secondary identification document.

Any document produced by the customer must be current.

D. Record of Verification of identity - individuals

A completed Know-Your-Client Evidence Verification Form is to be held on a file along with a copy of the original application completed by the individual.

A mark must be made alongside the customer's name, residential address and date of both on the form to evidence that the information is consistent with the customer provided identity documents. This mark may be either the signature or initials of the processing officer.

It is permissible to store an electronic image of the checklist and certified document in a format that may not be modified or edited.

E. On-going Due Diligence (KYC) requirements - individuals

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.1.2 Sole Traders

A. Identification information – sole traders

(1) the customer's full name;
(2) the customer's date of birth;
(3) the customer's residential address;
(4) the full business name (if any) under which the customer carries on his or her business;
(5) the full address of the customer's principal place of business (if any) or the customer's residential address; and
(6) any business number issued to the customer.

B. Verification of information - sole traders

The following information must be verified for each sole trader from customer provided identity documents (see paragraph C. Identity documents – individuals):

(1) the customer's full name; and
(2) either:
(a) the customer's date of birth; or
(b) the customer's residential address.

C. Identity documents – sole traders

Acceptable documents listed in the Know-Your-Client Evidence Verification Form.
Acceptable documents are:

(a) an original or certified copy of a primary photographic identification document; or
(b) both:
(i) an original or certified copy of a primary non-photographic identification document; and
(ii) an original or certified copy of a secondary identification document.

Any document produced by the customer must be current.

D. Record of Verification of identity – sole traders

(1) A completed Know-Your-Client Evidence Verification Form is to be held on a file along with a copy of the original application completed by the individual.
A mark must be made alongside the customer's name, residential address and date of both on the form to evidence that the information is consistent with the customer provided identity documents. This mark may be either the signature or initials of the processing officer.

It is permissible to store an electronic image of the checklist and certified document in a format that may not be modified or edited.

(2) The business number and sole trader's name are to be confirmed by looking up the number and name

A print out of the business search is to be held on file confirming the business number and sole trader's name have been electronically verified.

E. On-going Due Diligence (KYC) requirements – sole traders

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.2 Companies

10.2.1 Domestic companies

A. Identification information – domestic companies

(1) the full name of the company as registered by the BVI;
(2) the full address of the company's registered office;
(3) the full address of the company's principal place of business, if any;
(4) the company number issued to the company;
(5) whether the company is registered by the BVI as a proprietary or public company;
(6) if the company is registered as a proprietary company, the name of each director of the company; and
(7) the name and address of each beneficial owner of the company (applies only for unlisted companies).

B.1. Verification of information - domestic companies (Unlisted)

These verification requirements apply to registered companies that are not:

(1) a domestic listed public company;
(2) a majority owned subsidiary of a domestic listed public company; or

(3) licensed and subject to the regulatory oversight of a commonwealth, state or territory statutory regulator in relation to its activities as a company.

Confirm the following based on the provided company business number through an BVI business register search:

(a) the full name of the company as registered by the BVI;
(b) whether the company is registered in the BVI as a proprietary or public company; and
(c) the company number issued to the company.

In addition to the verification of company information, the identities of beneficial owners of an unlisted company must also be verified (see paragraph D. Record of Verification of identity - registered companies)

B.2 Verification of information - domestic companies (Listed & Government Regulated)

These verification requirements apply to BVI registered companies which are either:

(1) a domestic listed public company;
(2) a majority owned subsidiary of a domestic listed public company; or
(3) licensed and subject to the regulatory oversight of a commonwealth, state or territory statutory regulator in relation to its activities as a company.

Obtain one or a combination of the following:

(a) a search of the relevant domestic stock exchange;
(b) a public document issued by the relevant company;
(c) a search of the relevant business database; or
(d) a search of the licence or other records of the relevant regulator.

C.1 Identity documents –registered companies (Unlisted)

A document to be titled 'Disclosure Certificate' must be provided which lists the name and address of each beneficial owner of the unlisted company.

C.2 Identity documents – registered companies (Listed & Government Regulated)

No identity documents are required to be produced by the customer unless enhanced due diligence procedures apply (see paragraph E - On-going Due Diligence (KYC) requirements –registered companies).

D. Record of Verification of identity - domestic companies

A copy of the database result is to be printed off and held on the applicant's file.

Verification documentation - domestic companies (Unlisted) – beneficial owners

All beneficial owners of an unlisted domestic company must be identified and verified.

A list of current shareholders in the company is to be provided by the applicant via a Disclosure Certificate (see clause 10).

In addition, the applicant will source and obtain the necessary information and verification documents appropriate to each shareholder.

The following referenced procedures will be followed depending on the nature of each shareholder:

Shareholder type	Identification and verification procedure – Paragraph Reference
Natural Person	10.1
Company	10.2
Trustee	10.3
Association	10.5
Government Body	10.7

E. On-going Due Diligence (KYC) requirements – registered companies

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.2.2 Registered foreign companies

A. Identification information –registered foreign companies

(1) the full name of the company as registered;
(2) the full address of the company's registered office;
(3) the full address of the company's principal place of business or the full name and address of the company's local agent in the BVI, if any;
(4) the business number issued to the company;
(5) the country in which the company was formed, incorporated or registered;

(6) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and
(7) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company.
(8) the name and address of each beneficial owner of the company (applies only for unlisted companies).

B. Verification of information –registered foreign companies

Confirm the following:

(1) the full name of the company as registered;
(2) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company; and
(3) the business number issued to the company.

In addition to the verification of company information, the identities of beneficial owners of a company must also be verified (see paragraph D. Record of Verification of identity - registered companies)

C. Identity documents – registered foreign companies

A Disclosure Certificate must be provided which contains information about whether the company is registered by the relevant foreign registration body and if so, whether it is registered as a private or public company or some other type of company.

If the company is an unlisted company, then the Disclosure Certificate must also list the name and address of each beneficial owner of the company.

D. Record of Verification of identity – registered foreign companies

A copy of the National Names Index database result is to be printed off and held on the applicant's file.

Verification documentation – beneficial owners of foreign companies (Unlisted companies only)

All beneficial owners of unlisted foreign companies must be identified and verified where possible.

A list of current shareholders in the company is to be provided by the applicant via a Disclosure Certificate (see paragraph 10).

A list of current shareholders in the company is to be provided by the applicant.

In addition, the applicant will source and obtain the necessary information and verification documents appropriate to each shareholder. The following referenced procedures will be followed depending on the nature of each shareholder:

Shareholder type	Identification and verification procedure – Paragraph Reference
Natural Person	10.1
Company	10.2
Trustee	10.3
Association	10.5
Government Body	10.7

E. On-going Due Diligence (KYC) requirements – registered companies

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.2.3 Foreign companies not registered

A. Identification information – foreign companies not registered

(1) the full name of the company;
(2) the country in which the company was formed, incorporated or registered;
(3) whether the company is registered by the relevant foreign registration body and if so:
    (i) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;
    (ii) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and
    (iii) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;
(4) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company; and
(5) if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

(6) the name and address of each beneficial owner of the company (applies only for unlisted companies).

B. Verification of information - foreign companies not registered

The relevant registration authority is to be contacted and the identity of the unregistered foreign company is to be confirmed. Confirmation may be made by letter or email issued by a responsible person within the authority, or by searching a web based public database maintained by the authority.

This search is to confirm:

(1) the full name of the company; and
(2) whether the company is registered by the relevant foreign registration body and if so:
(i) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration; and
(ii) whether the company is registered as a private or public company.

C. Identity documents – foreign companies not registered

A Disclosure Certificate must be provided which sets out:

(1) the full name of the company; and
(2) whether the company is registered by the relevant foreign registration body and if so:
(a) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;
(b) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body; and
(c) the jurisdiction of incorporation of the foreign company as well as the jurisdiction of the primary operations of the foreign company and the location of the foreign stock or equivalent exchange (if any); and
(d) contain the full name and full residential address of each beneficial owner.
(3) if the company is unlisted, the name and address of each beneficial owner of the company.

D. Record of Verification of identity – foreign companies not registered

A copy of the written verification or database search result is to be held on file, along with any copies of incorporation or registration documentation provided by the customer.

Verification documentation – beneficial owners of foreign companies (unlisted companies only)

All beneficial owners of unlisted foreign companies must be identified and verified where possible.

A list of current shareholders in the company is to be provided by the applicant. In addition, the applicant will source and obtain the necessary information and verification documents appropriate to each shareholder. The following referenced procedures will be followed depending on the nature of each shareholder:

Shareholder type	Identification and verification procedure – Paragraph Reference
Natural Person	10.1
Company	10.2
Trustee	10.3
Association	10.5
Government Body	10.7

E. On-going Due Diligence (KYC) requirements – foreign companies not registered

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.3 Trustees

10.3.1 Non-exempt Trustees

These procedures relate to 'non-exempt trustees'. Non-exempt trustees are defined to include trustees of all trusts, with the exceptions of the following types of schemes:

(1) a managed investment scheme that is registered;
(2) a managed investment scheme that is not registered and that:
    (a) only has wholesale customers; and
    (b) does not make small scale offerings;
(3) a trust registered with and subject to the regulatory oversight of a statutory regulator in relation to its activities as a trust; or
(4) a government retirement fund established by legislation.

Examples non-exempt trustees include the following types of schemes:

(1) Small regulated retirement funds

(2) Family trusts
(3) Unregistered managed investment schemes which have Retail Clients who have been issued interests under the small-scale offerings exemption.

A. Identification information – non-exempt trustees

(1) the full name of the trust;
(2) the full business name of the trustee in respect of the trust, if any;
(3) the type of the trust;
(4) the country in which the trust was established;
(5) if any of the trustees is an individual, then in respect of those individuals:
    (a) the trustee's full name;
    (b) the trustee's date of birth; and
    (c) the trustee's residential address;
(6) if any of the trustees is a company, then in respect of those companies:
    (a) the full name of the company as registered;
    (b) the full address of the company's registered office;
    (c) the full address of the company's principal place of business, if any;
    (d) the business number issued to the company;
    (e) whether the company is registered as a proprietary or public company;
    (f) if the company is registered as a proprietary company, the name of each director of the company; and
    (g) the name and address of each beneficial owner of the company; and
(7) the full name of each beneficiary in respect of the trust; or
(8) a description of each class of beneficiary under the trust.

B. Verification of information - non-exempt trustees

(1) Confirmation of the business number

(2) Where the trustee is, or includes, a company, confirm the following:
    (a) the full name of the company as registered;
    (b) whether the company is registered as a proprietary or public company; and
    (c) the company number issued to the company.

(3) Where the trustee is, or includes, natural persons the following information must be verified for each individual from customer provided identity documents (see paragraph C. Identity documents – non-exempt trustees):
(i) the individual's full name; and
(ii) either:
    (a) the individual's date of birth; or
    (b) the individual's residential address.

C. Identity documents – non-exempt trustees

(1) A certified copy of the trust deed for the trust, demonstrating that the trustee has been appointed under the instrument, or

(2) Where it is not possible to obtain a certified copy of the trust's deed, then a document to be titled 'Disclosure Certificate' must be provided which sets out the:

(a) name(s) of the trustee(s)
(b) if a corporate trustee, whether the company is registered as a proprietary or public company and its company number.

The Disclosure Certificate must be signed or otherwise authenticated by a director, company secretary, appointed AML/CTF Compliance Officer of the company (if appointed) or an equivalent officer of the company (such as a Compliance Officer).

The Disclosure Certificate may be made as a letter, using the term 'Disclosure Certificate' in the title header.

(3) For trustees who are natural persons:

(a) an original or certified copy of a primary photographic identification document; or
(b) both:
(i) an original or certified copy of a primary non-photographic identification document; and
(ii) an original or certified copy of a secondary identification document.

Any document produced by the individual must be current.

(4) Additional identity documents may be required to be obtained from the customer if enhanced due diligence procedures apply (see paragraph E - On-going Due Diligence (KYC) requirements – non-exempt trustees).

D. Record of Verification of identity - non-exempt trustees

(1) confirmation of the business number and trust name
(2) where the trustee is, or includes, a company, a copy of the National Names Index database result is to be printed off and held on file;
(3) where the trustee is, or includes, a natural person - a completed Know-Your-Client Evidence Verification Form is to be held on a file for each natural person who is a trustee. A mark must be made alongside the individual's name, residential address and date of both on the form to evidence that the information is consistent with the customer provided identity documents. This mark may be either the signature or initials of the processing officer.

It is permissible to store an electronic image of the checklist and certified document in a format that may not be modified or edited;

(4) a certified copy of the trust's deed; or
(5) a 'Disclosure Certificate' and
(6) a list of beneficiaries' names or the description of the class of beneficiaries provided for under the trust.

E. On-going Due Diligence (KYC) requirements – non-exempt trustees

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.3.2 Exempt Trustees

These procedures relate to 'exempt trustees'. Exempt trustees are defined here to include trustees of following types of schemes:

(1) a managed investment scheme registered;
(2) a managed investment scheme that is not registered and that:
    (a) only has wholesale customers; and
    (b) does not make small scale offerings
(3) registered and subject to the regulatory oversight of a statutory regulator in relation to its activities as a trust; or
(4) a government retirement fund established by legislation.

A. Identification information – Exempt trustees

(1) the full name of the trust;
(2) the full business name (if any) of the trustee in respect of the trust;
(3) the type of the trust;
(4) in the case of a registered managed investments scheme, the scheme's registered scheme number;
(5) in the case of an unregistered managed investments scheme which has and does not make small scale offerings – financial services licence number of the trustee and a written statement from the trustee stating that no Retail Clients are held within the scheme;
(6) in the case of a government retirement fund established by legislation, a statutory declaration or other written evidence that it is the trustee of such a fund.

B. Verification documentation - Exempt trustees

(1) In the case of a registered managed investments scheme, confirm the scheme's name and number by looking up the relevant National Names Index database.
(2) In the case of any other trustee, conduct any such reasonable searches to verify the information provided.

C. Identity documents –Exempt trustees

No identity documents are required to be produced by an exempt trustee.

Additional identity documents may be required to be obtained from the customer if enhanced due diligence procedures apply (see paragraph E - On-going Due Diligence(KYC) requirements –Exempt trustees).

D. Record of Verification of identity - Exempt trustees

(1) in the case of registered managed investments scheme, print off and retain on file a copy of the search results from the relevant National Names Index database;
(2) in the case of any other trustee, holding on file copies of any documents obtained through the search confirming the identity of either the trustee or fund.

E. On-going Due Diligence (KYC) requirements – Exempt trustees

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

Depending on the circumstances, and the information already held by BCR, the additional KYC information sought may be those matters listed in section 7.2.

10.4 Partnerships

A. Identification information – Partnerships

(1) the full name of the partnership;
(2) the full business name (if any) of the partnership as registered under any State or Territory business names legislation;
(3) the country in which the partnership was established;
(4) in at least of the partners who is a natural person
    (a) the partner's full name;

(b) the partner's date of birth; and
(c) the partner's residential address.

(5) In the case of a US regulated limited liability partnerships ('LLP'), the full name and address of the General Partner and the US State of registration of the LLP.

B. Verification of information – Partnerships

(1) Confirmation of the full name of the partnership from a partnership agreement or of minutes of a partnership meeting.
(2) For one of the partners who is a natural person, the following information must be verified for each individual from customer provided identity documents (see paragraph C. Identity documents –Partnerships):
(i) the individual's full name; and
(ii) either:
(a) the individual's date of birth; or
(b) the individual's residential address.

C. Identity documents – Partnerships

(1) A partnership agreement, certified copy or certified extract of a partnership agreement;
(2) A certified copy or certified extract of minutes of a partnership meeting; or
(3) Where it is not possible to obtain a certified copy or certified extract of a partnership agreement or minutes, then a Disclosure Certificate must be provided which sets out the:
(a) full name of the partnership, and
(b) confirmation that the individual to be identified is a partner of the partnership.

The Disclosure Certificate must be signed or otherwise authenticated by a partner of the partnership.

The Disclosure Certificate may be made as a letter, using the term 'Disclosure Certificate' in the title header.

(4) For partner who is natural person and who has been identified for verification per paragraph A. Identification information – Partnerships:
(a) an original or certified copy of a primary photographic identification document; or
(b) both:
(i) an original or certified copy of a primary non-photographic identification document; and
(ii) an original or certified copy of a secondary identification document.

Any document produced by the individual must be current.

Record of Verification of identity - Partnerships

Copies of the partnership agreement and/or minutes are be appended to held on file.

Where a 'Disclosure Certificate' has been provided instead of a copy or extract of either the partnership agreement and/or minutes, then the Disclosure Certificate must be held on file.

A completed Know-Your-Client Evidence Verification Form is to be held on a file along for any individual whose identity has been verified.

A mark must be made alongside the individual's name, residential address and date of both on the form to evidence that the information is consistent with the customer provided identity documents. This mark may be either the signature or initials of the processing officer.

It is permissible to store an electronic image of the checklist and certified document in a format that may not be modified or edited.

E. On-going Due Diligence (KYC) requirements - Partnerships

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

10.5 Incorporated and unincorporated associations

A. Identification information – associations

(1) the full name of the association;
(2) the full address of the association's principal place of administration or registered office (if any) or the residential address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer;
(3) if incorporated, any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association;
(4) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and
(5) for unincorporated associations, in respect of the chairman, secretary and treasurer or equivalent officer:
    (a) the member's full name;
    (b) the member's date of birth; and
    (c) the member's residential address.

B. Verification of information – associations

(1) For incorporated associations:

Verify from a State, Territory or overseas body responsible for the incorporation of the association or from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data:

(a) the full name of the incorporated association; and
(b) any unique identifying number issued to the incorporated association upon its incorporation.

(2) For unincorporated associations:

(a) verify the full name (if any) of the association from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data; and
(b) the following information must be verified for the chairman, secretary and treasurer or equivalent officer from the provided identity documents (see paragraph C. Identity documents – Associations):

(1) the individual's full name; and
(2) either:
(i) the individual's date of birth; or
(ii) the individual's residential address.

C. Identity documents – associations

(1) the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;

(2) the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association; or

(3) Where it is not possible to obtain a certified copy or certified extract of either the constitution\ rules or minutes, then a Disclosure Certificate must be provided which sets out the matters listed under paragraph A. Identification information – associations.

The Disclosure Certificate must be signed or otherwise authenticated by achairman, secretary or treasurer or AML/CTF Compliance Officer or equivalent officer of the association (such as a Compliance Officer).

The Disclosure Certificate may be made as a letter, using the term 'Disclosure Certificate' in the title header.

(4) In the cases of an unincorporated association, acceptable identity documents listed in the Know-Your-Client Evidence Verification Form for each of the chairman, secretary and treasurer or equivalent officer. The usual acceptable identity documents are:

(a) an original or certified copy of a primary photographic identification document; or
(b) both:
(i) an original or certified copy of a primary non-photographic identification document; and
(ii) an original or certified copy of a secondary identification document.

Any document produced by the customer must be current.

D. Record of Verification of identity - associations

(1) Copies of the constitution/rules or minutes obtained per above are to be appended to the application file.
(2) Where it has not been possible to obtain copies of the constitution/rules or minutes, then a Disclosure Certificate must be provided. (2) In the case of unincorporated associations, a completed Know-Your-Client Evidence Verification Form for each of the chairman, secretary and treasurer or equivalent officer is to be held on a file along with a copy of the original application completed by the individual.
A mark must be made alongside the customer's name, residential address and date of both on the form to evidence that the information is consistent with the customer provided identity documents. This mark may be either the signature or initials of the processing officer.

It is permissible to store an electronic image of the checklist and certified document in a format that may not be modified or edited.

E. On-going Due Diligence (KYC) requirements - associations

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

10.6 Registered co-operatives

A. Identification information – registered co-operatives

(1) the full name of the co-operative;

(2) the full address of the co-operative's registered office or principal place of operations (if any) or the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer;

(3) any unique identifying number issued to the co-operative upon its registration by the State, Territory or overseas body responsible for the registration of the co-operative; and

(4) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative.

B. Verification of information – registered co-operatives

Verify from information provided by the State, Territory or overseas body responsible for the registration of the co-operative or from any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative or from reliable and independent documents relating to the co-operative or from reliable and independent electronic data:

(a) the full name of the co-operative; and

(b) any unique identifying number issued to the co-operative upon its registration.

C. Identity documents - registered co-operatives

(1) any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative;

(2) any minutes of meeting of the co-operative or a certified copy or certified extract of any minutes of meeting of the co-operative; or

(3) information provided in written form by or extract from a State, Territory or overseas body responsible for the registration of the co-operative; or

(4) where it has not been possible to obtain copies of the above, then then a

Disclosure Certificate must be provided which sets out the matters listed under paragraph A. Identification information – registered co-operatives.

The Disclosure Certificate must be signed or otherwise authenticated by achairman, secretary or treasurer or AML/CTF Compliance Officer or equivalent officer of the association (such as a Compliance Officer).

The Disclosure Certificate may be made as a letter, using the term 'Disclosure Certificate' in the title header.

D. Record of Verification of identity – registered co-operatives

Copies of any register, minutes, written advice or extract obtained per above is to be held on file.

E. On-going Due Diligence (KYC) requirements - registered co-operatives

These requirements apply where a customer's identity is suspected to be false (see section 7.2.1).

Where a customer's identity is suspected the AML/CTF Compliance Officer will be notified. The AML/CTF Compliance Officer will then agree the additional information and enquiries that will be undertaken to complete the enhanced customer due diligence (see section 7.2.3).

Discrepancies identified through the verification process may give rise to enhanced customer due diligence.

10.7 Government bodies

A. Identification information – Government bodies

(1) the full name of the government body;
(2) the full address of the government body's principal place of operations;
(3) whether the government body is an entity or emanation, or is established under legislation; and
(4) whether the government body is an entity or emanation, or is established under legislation, of a State, Territory, or a foreign country and the name of that State, Territory or country.

B. Verification of information – Government bodies

Verify from a web search or other means all the information listed above.

C. Identity documents – Government bodies

(1) None required for BVI Government bodies.

(2) For foreign Government bodies a letter on departmental letter head is to be obtained.

D. Record of Verification of identity – Government bodies

Copies of extracts provided from web search to be held on file. In the case of a foreign

Government, a copy of a letter on departmental letter head.

10.8 Beneficial Owner Information

The following identification information and verifications are required to be undertaken for beneficial owners of [Name's] customers:

A. Identification information – Beneficial Owners

(1) each beneficial owner's full name, and
(2) the beneficial owner's date of birth; or
(3) the beneficial owner's full residential address.

B. Verification of information – Beneficial owners

The beneficial owner's full name and either the beneficial owner's full residential addressor date of birth, or both. The usual acceptable identity documents are:

(1) an original or certified copy of a primary photographic identification document; or
(2) both:
(i) an original or certified copy of a primary non-photographic identification document; and
(ii) an original or certified copy of a secondary identification document.

Any document produced by the customer must be current.

C. Procedure where unable to determine the identity of the beneficial owner

If BCR is unable to ascertain a beneficial owner, it must identify and take reasonable measures to verify:

(1) for a company (other than a company which is verified under the simplified company verification procedure) or a partnership, any individual who:
a. is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or
b. holds the position of senior managing official (or equivalent);

(2) for a trust (other than a trust which is verified under the simplified trustee verification procedure) any individual who holds the power to appoint or remove the trustees of the trust:

(3) for an association or registered co-operative, any individual who:
a. is entitled (either directly or indirectly) to exercise 25% or more of the voting rights including a power of veto, or
b. would be entitled on dissolution to 25% or more of the property of the association or registered co-operative, or
c. holds the position of senior managing official (or equivalent).

In addition, BCR may be able to use a Disclosure Certificate. See clause 10 of Part A for further details.

10.9 Politically Exposed Person Information

The following identification information and verifications are required to be undertaken to determine whether a customer or beneficial owner is a politically exposed person:

(1) for domestic politically exposed persons and international organisation politically exposed persons:

a. in the case of a beneficial owner, comply with the identification requirements in clause 10.1 as if the politically exposed person was the customer; and
b. determine whether the person is of high ML/TF risk; and
c. if the person is determined to be of high ML/TF risk, then in addition, carry out the steps in clause 10.9(2).
d. for foreign politically exposed persons and for high ML/CT risk domestic or international organisation politically exposed persons:
e. in the case of a beneficial owner, comply with the identification requirements in clause 10.1 as if the politically exposed person was the customer; and
f. obtain senior management approval before establishing or continuing a business relationship with the individual and before the provision, or continued provision, of a designated service to the customer;
g. take reasonable measures to establish the politically exposed person's source of wealth and source of funds; and
h. comply with the ongoing customer due diligence procedures in clause 7.2.

11. Agents of customers

In some cases, a customer may appoint an agent to contract for a designated service. In financial services, examples of such agencies include appointing an Attorney to conduct the affairs of the principal, or where a foreign corporation establishes a local representative office to facilitate services on its behalf.

The AML/CTF Code contemplates two types of such agents:

(1) Natural persons; and
(2) Corporations.

11.1 Agents who are natural persons

A. Identification information – agents who are natural persons

In providing a service to a customer through an agent who is a natural person(s), BCR is required to obtain:

(1) the full name(s) of the agent(s), and
(2) obtain evidence of the appointment of the agent(s).

B. Verification documentation – agents who are natural persons

It will be necessary to obtain a certified copy of a Power of Attorney or other such instrument appointing an agent.

C. Record of Verification of identity – agents who are natural persons

The name of the agent must be retained along with the application file, along with a copy of the instrument appointing the agent.

11.2 Agents who are corporations

Where the agent is a corporation, the Commission Code permit the identity of an incorporated agent to be verified by an officer of the customer.

The Verifying Officer may be an employee, agent or contractor of the customer. In such a case BCR is to be provided with a copy of the written appointment of the Verifying Officer made by the customer.
The Verifying Officer has to be verified by BCR per the procedures set out in section 10.1 of this Part B.

Then the Verifying Officer is to provide the following to BCR:

(a) the full name of the agent
(b) The title of the position or role held by the agent with the customer
(c) a copy of the signature of the agent; and
(d) evidence of the agent's authorisation to act on behalf of the customer.

12. Certification of documents

Documents provided for the purposes of verifying the identities of either customers or agents of customers must either be original or certified copies.

Documents may only be certified by the following types of persons:

(1) a person who is enrolled on the roll of the Supreme Court of a commonwealth, state or territory, as a legal practitioner (however described);
(2) a judge of a court;
(3) a magistrate;
(4) a chief executive officer of a court;
(5) a registrar or deputy registrar of a court;
(6) a Justice of the Peace;
(7) a Notary Public;
(8) a police officer;
(9) an officer with 2 or more continuous years of service with one or more financial institutions;
(10) a finance company officer with 2 or more continuous years of service with one or more finance companies (for the purposes of the Statutory Declaration Regulations 1993);
(11) an officer with, or authorised representative of, a holder of an BVI financial services licence, having 2 or more continuous years of service with one or more licensees; or

It is advisable that any certification provided on a document provided is made in the following or similar format:

I certify that this is a true copy of the original document:

Signature

Printed Name

Title/Position

Date

13. Electronic Checks

As an alternative or supplementary to documentary evidence of identity, the applicant's identity, date of birth, or address and other available information may be checked electronically by accessing other data-bases or sources. Each source may be used separately as an alternative to one or more documentary checks.

In respect of electronic checks, confidence as to the reliability of information supplied will be established by the cumulative nature of checking across a range of sources, preferably covering a period of time or through qualitative checks that assess the validity of the information supplied. The number or quality of checks to be undertaken will vary depending on the diversity as well as the breadth and depth of information available from each source. Verification that the applicant is the data-subject also needs to be conducted within the checking process.

13.1 BCR's Permissions

BCR is permitted to:

1. Disclose the identification information – specifically, one or more of an individual's name, residential address and date of birth – to an Electronic Verification Company.

    - Transaction history is not permitted to be used in relation to this method of verification.

2. Use the assessment provided by the Electronic Verification Company. which indicates whether the identification information provided by the reporting entity matches the information held by it on its credit information files, to verify a customer's or other individual's identity for the purposes of the AML/CTF Code.

    - As the assessment from the Electronic Verification Company must contain an aggregate score or ranking to indicate the level or degree of match of the information, reporting entities will need to determine, in conjunction with their risk analysis under their AML/CTF program,

whether a CRA's assessment will be considered sufficient for verification of the identity of the individual.

13.2 BCR's Requirements

BCR is required to:

1. Obtain express and informed consent from an individual, as set out in the AML/CTF Code, prior to making a verification request:

   - The concept of express consent is not defined in the Privacy requirements. For the purposes of this Manual, it means that the individual must actively agree to a reporting entity verifying their identity against personal information obtained by an Electronic Verification Company. A reporting entity cannot rely on implied consent (where agreement is taken to have occurred based on the absence of evidence of disagreement).

   - Express consent can be indicated online, or on the phone. However, records must be retained to evidence the process followed and the consent given by the individual.

   - To ensure that the consent is informed, the consent must be specifically about the disclosure of personal information by the reporting entity to the Electronic Verification Company and use by the Electronic Verification Company of the personal information contained in credit information files for an assessment. The consent will specify that the reporting entity will only use the assessment by the reporting entity for the purpose of verifying the individual's identity for the purposes of the AML/CTF Code: a general consent to the use of information to verify identity will not be sufficient. If an individual other than the customer is being identified, that person will also have to consent to the process.

   - To ensure that the consent is genuine, the AML/CTF Code requires that the individual must be given another option, not reliant upon credit reporting information, for verifying their identity. This will ensure that those who choose not to use their credit information file for this purpose, or those who do not have a credit information file, are not disadvantaged when seeking to obtain designated services.

2. Notify the individual of a failure to verify the information in a written notice, if the assessment from the Electronic Verification Company does not enable the reporting entity to verify an individual's identification information, as set out in the AML/CTF Code. Written notice includes a notice delivered electronically, such as by email.

3. Retain a record containing specified information relating to a verification request. As set out in the AML/CTF Code, a reporting entity must retain this information for a period starting from the date of the verification request and ending 7 years after the reporting entity ceased providing a

designated service to the individual, and must delete it at the end of that period. This retention period is consistent with other record keeping obligations under the AML/CTF Code, and will enhance the level of transparency of the verification processes by ensuring that records can be reviewed to ensure compliance with the relevant requirements and to enable individuals to obtain access to verification requests and the outcomes of any assessments.

[End of Part B]

1.