Financial Intelligence Centre

DRAFT PUBLIC COMPLIANCE COMMUNICATION

DRAFT PUBLIC COMPLIANCE COMMUNICATION 112 (Draft PCC112)

ON THE IDENTIFICATION OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS AND ASSOCIATED CUSTOMER DUE DILIGENCE FOR CLIENTS OF AUTHORISED USERS OF AN EXCHANGE IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT 38 OF 2001)

PCC SUMMARY

The counterparty, as client of an authorised user of an exchange (authorised user), is the person who provides the authorised user with a mandate. An authorised user must first identify the money laundering and terrorist financing (ML/TF) risks their client, being the counterparty, presents prior to determining if they will continue with any arrangement with the client.

There are three (3) scenarios in respect of how an authorised user can interact with their clients, or counterparties in this document, namely a direct interaction with a client, an indirect interaction with a client, and a direct interaction where there is a counterparty and the *client* of the counterparty involved.

An authorised user does not have a customer due diligence (CDD) obligation towards the *client* of the counterparty. However, in order for the authorised user to effectively understand the ML/TF risks associated with its client, as counterparty, sufficient information needs to be obtained by the authorised user about the *client* of their counterparty.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Centre provides, does not relieve the user of the guidance from the responsibility to exercise their own skill and care in relation to the user's legal position. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

COPYRIGHT NOTICE

OBJECTIVE

The objective of this draft PCC is to assist authorised users in applying effective risk management and customer due diligence (CDD) in engagements with their clients.

GLOSSARY

"Authorised user" refers to an authorised user of an exchange as referred to in Item 4 of Schedule 1 to the FIC Act

"*Client* of the counterparty" refers to the *client* of the counterparty, where the counterparty is an authorised user's client, and where the authorised user has not established a business relationship nor conducted a single once-off transaction with the *client* of the counterparty, either directly or indirectly.

"Counterparty" refers to the client of the authorised user, also the authorised user's client, who provides the authorised user with a mandate. The term counterparty in this draft PCC means the same as client, prospective client as the client of an authorised user.

"FIC Act" refers to the Financial Intelligence Centre Act, 2001 (Act 38 of 2001).

"**FSP"** refers to a financial services provider as defined in section 1 of the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002) (FAIS Act).

"**Foreign intermediaries**" refers to foreign individuals and/or institutions that conduct business similar to what is generally understood as the business of an FSP in South Africa, where such entities are neither authorised FSPs in terms of the FAIS Act, nor considered as accountable institutions in terms of the FIC Act.

"Intermediary" refers to the direct client of an authorised user where such a client does not act on its own behalf but on behalf of its clients.

"The Centre" means the Financial Intelligence Centre established in terms of section 2 of the FIC Act.

1. INTRODUCTION

1.1. This PCC is intended for authorised users of an exchange as referred to in item 4 of Schedule 1 to the FIC Act.

1.2. This PCC seeks to assist authorised users in applying effective risk management and CDD in direct and/or indirect engagements with their clients, as counterparties.

1.3. An authorised user must first assess the ML/TF risk posed by a counterparty to a transaction or business relationship before they can determine whether to enter into any arrangement with this client, and similarly prior to the booking of any trade. In so doing, disruption or interruption to stock broking trade will be limited.

2. CLIENT DETERMINATION AND ML/TF RISK ASSESSMENT

2.1. A person who has entered into a business relationship or a single transaction with an accountable institution is considered to be the counterparty, or client of an accountable institution. An authorised user must determine who its client is during the on-boarding stage.

2.2. The authorised user's risk management and compliance programme (RMCP) must provide for the manner in which the institution determines if a person is a client or a prospective client.

2.3. An authorised user must understand and assess the ML/TF risks introduced by each of its clients. As part of understanding and assessing the ML/TF risks that the authorised user's client presents holistically, the authorised user must understand and assess what inherent ML/TF risks the *client* of the counterparty presents.

2.4. There are three (3) scenarios in respect of how an authorised user can interact with their clients, each of which having associated CDD compliance requirements. Firstly, where a client engages and enters into a business relationship or transaction directly with an authorised user and indirectly through representation by a third party or indirectly on behalf of a third party. Lastly, the direct client of the authorised user may have their own *clients*

that are not party to the transaction and or business relationship between the authorised user and the authorised users' client. The below diagram sets out these scenarios:

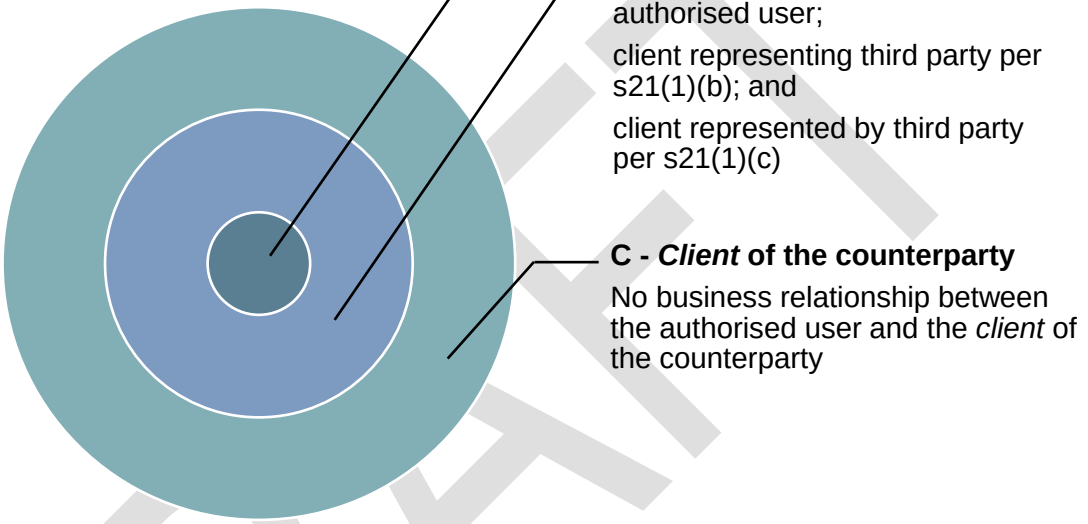

Image 1 Scenario of direct and indirect interaction with clients

2.5. The above scenarios will assist the authorised user in determining who their clients are, and to ascertain the level of information required to determine the ML/TF risk and the required level of CDD, where applicable, to be applied in respect of their client as the counterparty and the *client* of the counter party.

2.6. An authorised user has CDD obligations in respect of clients who are onboarded either in direct engagement with a client (scenario A) and/or in an indirect engagement with a client (scenario B), as expressed in section 21(1)(a), 21(1)(b) and 21(1)(c) of the FIC Act.

2.7. It can occur that there is a direct relationship between the authorised user and their client, where the authorised user's client is controlling funds on behalf of the *client* of the counterparty (scenario C). The authorised user has a CDD obligation towards their client

and in fulfilling this obligation they must obtain sufficient information about the *client* of the counterparty in order to identify and assess the ML/TF risk that the authorised user's client, as counterparty, presents.

2.8. The inherent risk that the *client* of the counterparty presents to the authorised user can be taken into account as part of the client risk indicator, (refer to Guidance Note 7, which sets out the various indicators that should be taken into account when assessing the ML/TF risk a client as counterparty presents).

Example 1: Basic practical scenarios as listed in image 1

Scenario A

Client establishes a business relationship and or conducts a single once-off transaction with the authorised user directly. There is no FSP or foreign intermediary involved.

Scenario B

An FSP establishes a business relationship with an authorised user on behalf of the authorised user's client. The client is both a client of the FSP and the authorised user.

Or

The client establishes a relationship with the authorised user, on behalf of another person, and acts according to the instruction of that other person.

Scenario C

The underlying client instructs an FSP to buy or sell listed instruments or have agreed a discretionary portfolio management with an FSP. The FSP places an order to buy/sell listed instruments with an investment provider (another FSP). The investment provider establishes a relationship with the authorised user. The authorised user executes transactions on a stock exchange on the instructions of the investment provider. There is no business relationship between the *client* of the counterparty and the authorised user.

(Note that this would also be applicable when dealing with a foreign intermediary instead of an FSP)

2.9. It is the Centre's recommendation that authorised users should avoid establishing a business relationship with a foreign intermediary, where that foreign intermediary has no information available on its *clients (*ie. no information of the *client* of the counterparty*)*. This would present a heightened ML/TF risk. The authorised user, however, retains the discretion to decide with whom it establishes a business relationship based upon its risk appetite and risk-based approach. The authorised user remains liable for any non-compliance with the FIC Act that stems from such business relationships and/or single transactions.

2.10. See the Centre's Guidance Note 7 {insert link} for a detailed discussion on the risk-based approach and other customer due diligence (CDD) considerations.

3. UNDERSTANDING THE ML/TF RISK ASSOCIATED WITH THE *CLIENT* OF THE COUNTERPARTY

3.1. In order for the authorised user to have a full understanding of the ML/TF risk that is present in the relationship and/or transaction, they are to identify the risks that their client, either as a direct client, or as a counterparty, brings. Included in this determination is the ML/TF risks posed by the *client* of the counterparty.

3.2. Although the authorised user does not have a CDD obligation in respect of the *client* of the counterparty, they would need to obtain sufficient information about the *client* of the counterparty in order to understand the risk associated to the authorised user's client (counterparty).

3.3. The information pertaining to the *client* of the counterparty obtained from the authorised user's client would differ for each type of client and business relationship. Such information could be sourced from the counterparty's onboarding processes and CDD criteria that they apply to their *clients* (ie. *client* of the counterparty*).* This information could include:

3.3.1. Information regarding the nature of the *client* of the counterparty, e.g. legal persons, natural person whether it is a pension fund, an insurer or a Collective Investment Scheme (CIS) manager;

3.3.2. Whether the counterparty conducts business with domestic prominent influential persons or foreign prominent public officials;

3.3.3. Whether the counterparty scrutinises client information for sanctions purposes, and if any *clients* of the counterparty matched on a South African sanction's regime list (see guidance note 6A);

3.3.4. The processes and procedures relating to CDD, including ongoing client monitoring, followed by the counterparty on the *client* of the counterparty;

3.3.5. Whether the counterparty is registered with an appropriate authority;

3.3.6. Compliance by the counterparty with other anti-money laundering and terror financing obligations such as record-keeping, training, reporting and the use of a RMCP;

3.3.7. Whether the counterparty has an effective and efficient process for understanding and assessing the ML/TF risk the *client* of the counterparty presents, as well as the results of such risk assessment;

3.3.8. The AML/CTF regime that applies where the counterparty resides, in the case of foreign business, or from where business is received;

3.3.9. The perceived levels of organised crime and corruption and the regulatory regime in the country of origin, in the case of foreign business, or from where business is received;

3.3.10. Whether secrecy provisions apply to the jurisdiction in the case of foreign business;

3.3.11. Whether the counterparty would be willing and able to disclose the names and details of the *clients* of the counterparty, upon request;

3.3.12. Whether the *client* of the counterparty makes use of cash payments; and

3.3.13. The distribution channels and marketing strategies used by the counterparty and the risks associated with other institutions that are part of this value chain.

4. PRACTICAL APPLICATION OF CDD ON AUTHORISED USER'S CLIENTS

4.1. The practical CDD application in relation to the three (3) scenarios of authorised user interactions with client's, as summarised in image 1, are expanded on below:

Scenario A

4.1.1 The client is the direct client of the authorised user, the authorised user must assess the client's ML/TF risk and conduct CDD in respect of that client, in accordance with section 21(1)(a) of the FIC Act, and the authorised user's RMCP.

Example 1

Client X who is a registered Company, in their own name using their own funds goes to Authorised User A to purchase listed instruments of Company B. Authorised User A must determine the risk associated with Company X and must complete the required CDD for Company X including required beneficial ownership, as company X is a legal person.

Company X did not establish the business relationship with Authorised User A through an FSP.

Scenario B

4.1.2 The authorised user must assess the ML/TF risk and conduct CDD on its client as the authorised representative/intermediary **and** the person on whose behalf the client is acting, in terms of section 21(1)(b) of the FIC Act as detailed in the authorised user's RMCP.

4.1.3 The authorised user must assess the ML/TF risk and conduct CDD on the person who is acting on behalf of the client as the authorised representative/intermediary **and** its client, in terms of section 21(1)(c) of the FIC Act as detailed the authorised user's RMCP.

Example 2

Client H acts on the behalf of person G to invest in exchange traded instruments using Authorised User K to perform the trade.

Client H has a mandate from person G. Authorised User K, in terms of section 21(1)(b) of the FIC Act has an obligation to understand the risk associated with both

Client H and person G, and to perform the required CDD on both Client H and person G in terms of their RMCP (Person G is the client of Authorised User K).

Example 3

FSP A acts on the behalf of client B to invest in exchange traded instruments using Authorised User C to perform the trading.

FSP A has a mandate from client B. Authorised User C, in terms of section 21(1)(c) of the FIC Act has an obligation to understand the risk associated with both FSP A and client B, and to perform the required CDD on both FSP A and client B in terms of their RMCP. (Client B is the client of Authorised User C)

Scenario C

4.1.4 The authorised user acts in accordance with its client's direct instructions to trade a specific instrument on the market. The authorised user is therefore not deemed to be acting on the instruction of another person/entity, but on the instruction of their client, the counterparty, directly.

4.1.5 In such an instance the *client* of the counterparty is not the client of the authorised user, and no CDD obligations arise in respect of the *client* of the counterparty. However, in order to determine the ML/TF risk associated to the authorised user's client, as counterparty, they must obtain sufficient information of the *client* of the counterparty in order to make such a determination.

Example 4

Asset Manager X requests Authorised User Y to execute a trade. The client of Asset Manager X is a pension fund. Authorised User Y would need to perform CDD on Asset Manager X as its client. Authorised User Y would not have to conduct CDD on Asset Manager X's clients. In order to determine Asset Manager X's ML/TF risk, Authorised User Y would need to obtain sufficient information about Asset Manager X's clients in order to make a determination on the ML/TF risk associated with Asset Manager X.

Example 5

Foreign Asset Manager M requests Authorised User K to execute a trade. The client of Foreign Asset Manager M is a pension fund. Authorised User K would need to perform CDD on Foreign Asset Manager M as its client. The Authorised User K would not have to conduct CDD on the Foreign Asset Manager M's clients. In order to determine Asset Manager M's ML/TF risk, Authorised User K would need to obtain sufficient information about the Foreign Asset Manager M's clients in order to make a determination of the risks of foreign Asset Manager M.

Where Foreign Asset Manager M cannot obtain sufficient information from its client, authorised user K must determine on a risk-based approach whether to continue or not to establish the business relationship.

5. APPLICATION OF PRINCIPLES CONTAINED IN THIS DRAFT PCC FOR OTHER ACCOUNTABLE INSTITUTIONS

5.1 Although this draft PCC is based on stock broking scenarios within the authorised user industry, accountable institutions can apply the principles contained in this draft PCC when they have comparable scenarios.

6. CONSULTATION

6.1. Before issuing guidance to accountable institutions, supervisory bodies and other persons regarding the performance and compliance by them of their duties and obligations in terms of the FIC Act or any directive made in terms of the FIC Act, the Centre must in accordance with section 42B of the FIC Act—

6.1.1. Publish a draft of the guidance by appropriate means of publication and invite submissions; and

6.1.2. Consider submissions received.

6.2. Commentators are invited to comment on the draft guidance by submitting only written comments via the online comments submission link only. Any questions or requests relating to this draft PCC112 may be sent to the FIC only at consult@fic.gov.za. Submissions will be received until **Wednesday, 10 March 2021**, by close of business.

7. COMMUNICATION WITH THE CENTRE

7.1 The Centre has a dedicated compliance contact centre geared to assist accountable and reporting institutions to understand their registration obligations in terms of the FIC Act. Please call the compliance contact centre on +2712 641 6000, and select option 1.

7.2 Compliance queries may also be submitted online by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx or visiting the Centre's website and submitting an online compliance query.

Issued By:
The Director
Financial Intelligence Centre
19 February 2021