Financial Intelligence Centre

PUBLIC COMPLIANCE COMMUNICATION

PUBLIC COMPLIANCE COMMUNICATION 52 (PCC52)

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 client of an authorised user of an exchange, is the person who provides the authorised user of an exchange (authorised user) with a mandate. An authorised user must first identify and assess the money laundering and terrorist financing (ML/TF) risks their client presents prior to determining if they will enter into a business relationship or single transaction with the client and perform the associated customer due diligence (CDD).

Where an authorised user determines that a client is an financial services provider (FSP), and this FSP has its own clients that are not party to the single transaction or business relationship, the authorised user must obtain sufficient information regarding the ML/TF risks of the FSPs client in order to identify and assess what inherent ML/TF risks the client (FSP) presents holistically.

DISCLAIMER

The publication of a PCC concerning any particular issue, as with other forms of guidance which the Financial Intelligence Centre (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 PCC is to assist authorised users in applying effective risk management and customer due diligence (CDD) in engagements with their clients.

GLOSSARY

"Accountable institution" refers to a person and/or entity as defined in Schedule 1 to the FIC Act

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

"FAIS Act" refers to the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002)

"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**" refer 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 applicable to authorised users of an exchange as referred to in item 4 of Schedule 1 to the FIC Act. The principles can be applied to comparable scenarios outside of authorised users' engagements, where applicable.

1.2. Authorised users must implement effective risk management and CDD in respect of all business relationships and single transactions with their clients.

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

2. CLIENT DETERMINATION AND ML/TF RISK ASSESSMENT

2.1. 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.

2.2. A person who has entered into a business relationship or a single transaction with an accountable institution is considered to be the client of an accountable institution, for the purposes of section 21 of the FIC Act. An authorised user must determine who its client is during the on-boarding stage.

2.3. For purposes of section 21(1)(b) and (c) of the FIC Act, where the client is acting on behalf of another person, or where another person is acting on behalf of the client, the authorised user must establish and verify the identity of both the client and that other person. Further, the authority to establish the business relationship or to conclude a single transaction on behalf of that other person or client must be established and verified.

2.4. An authorised user must understand and assess the ML/TF risks introduced by each of its clients and persons acting on behalf of their clients and other persons on whose behalf the client is acting on.

When a client is an FSP, who in turn has their own client(s) that are not party to the transaction or business relationship with an authorised user

2.5. It can occur that there is a single transaction or business relationship between the authorised user and their client (an FSP), where this FSP is controlling funds on behalf of this FSP's own client but where the client of the FSP is not a client of the authorised user.

2.6. The authorised user has a CDD obligation towards their client (FSP) and in fulfilling this obligation the authorised user must obtain sufficient information to identify and assess the ML/TF risks presented by the FSP's client, which in turn will assist in understanding and assessing the holistic ML/TF risk that the authorised user's client (FSP) presents.

2.7. Where the authorised user is not provided with sufficient information in order to adequately determine the ML/TF risk of their client, they will not be in a position to fulfil their CDD obligations set out in the FIC Act, and cannot proceed with the single transaction or business relationship, as read with section 21E of the FIC Act.

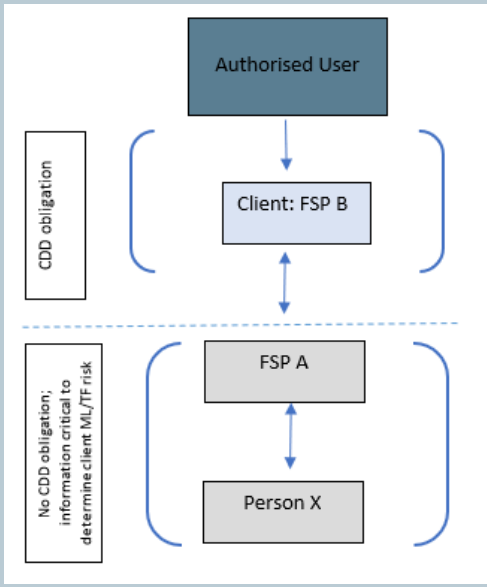
2.8. The inherent risk that the FSP's client presents to the authorised user can be taken into account as part of the client risk indicator, (refer to Guidance Note 7, part 11, which sets out the various indicators that should be taken into account when assessing the ML/TF risk a client presents).

Example 1: When the authorised users' client is an FSP, who in turn has their own clients

Person X instructs FSP A to buy or sell listed instruments or have agreed to a discretionary portfolio management with this FSP. FSP A places an order to buy/sell listed instruments with an investment provider (FSP B). The investment provider (FSP B) establishes a business relationship with the authorised user. The authorised user executes transactions on a securities exchange on the instructions of the investment

provider (FSP B). The authorised user identifies that FSP B is their client and that there is no business relationship between FSP Bs clients (FSP A or Person X) and the authorised user.

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



Note: all examples assume that the FSPs and authorised users act within their licensed activities.

2.9. The Centre strongly advises that authorised users consider the heightened ML/TF risk that they are exposing themselves to, by trading with foreign intermediaries that have little to no knowledge of who their own clients are. The authorised user remains liable for any non-compliance with the FIC Act or increased ML/TF risks that stem from such business relationships and/or single transactions.

2.10. See the Centre's Guidance Note 7, chapters 1 and 2 for a detailed discussion on the risk-based approach and other CDD considerations.

3. CLIENT ML/TF RISK DETERMINATION CONSIDERATIONS ASSOCIATED WITH AN FSP's CLIENT

This section is limited to the discussion of where the client (an FSP) of the authorised user has their own client (FSPs client) that are not party to the transaction or business relationship between the authorised user and the authorised users' client (the FSP).

3.1. For the authorised user to have a full understanding of the ML/TF risk that is present in a business relationship or single transaction with their client, they are to identify the ML/TF risks that their client (the FSP) brings. Included in this determination are the ML/TF risks posed by the FSP's client.

3.2. Although the authorised user does not have a CDD obligation in respect of the FSP's client, it needs to obtain sufficient information about the FSP's client in order to understand the risk associated with its client (the FSP).

3.3. The authorised user should request the information regarding the FSPs client(s) from the FSP. However, an authorised user is reminded that information pertaining to the FSP's client, so obtained from the FSP, would differ for each type of client and client engagement based on that FSPs client risk profiling.

3.4. The authorised user must, within its unique risk framework and risk appetite determine what information is to be obtained from its client (the FSP).

3.5. Examples of such information could include:

3.5.1. Information regarding the nature of the FSP's client, e.g. legal persons, natural person whether it is a pension fund, an insurer or a collective investment scheme (CIS) manager;

3.5.2. The FSPs business conducted with domestic prominent influential persons or foreign prominent public officials;

3.5.3. The FSPs level of scrutinising client information for sanctions purposes, and an undertaking that the FSP does not onboard any person that appears on a South African sanctions regime list (see guidance note 6A);

3.5.4. The processes and procedures relating to CDD, including ongoing client monitoring, followed by the FSP on its client;

3.5.5. The FSPs registration with an appropriate authority;

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

3.5.7. The level of effective and efficient processes for understanding and assessing the ML/TF risk the FSP's client presents, as well as the results of such risk assessment implemented by the FSP;

3.5.8. The ML/TF risk associated with the geographic area where the FSP resides, in the case of foreign business, or from where business is received;

3.5.9. The application of secrecy within the jurisdiction in the case of foreign business;

3.5.10. The use of cash by an FSP's client to facilitate trading instructions; and

3.5.11. The distribution channels used by the FSP and the risks associated with other institutions that are part of this value chain.

Note: the above considerations are applicable where the engagement is between a foreign intermediary and an authorised user, as with an FSP and authorized user, where appropriate.

3.6. The information regarding the client of the FSP must be obtained, assessed and included as part of the risk determination process of the client (FSP) at onboarding and on an ongoing basis as part of ongoing due diligence in respect of a business relationship as envisaged in section 21C of the FIC Act. Where the nature of the FSP's client or other relevant ML/TF risk factors change, this information must be provided to the authorised user to inform their ML/TF risk understanding of their client (the FSP). This may result in re-assessment of the client's (FSPs) ML/TF risk and the authorised user may be required to perform additional CDD where the ML/TF risk changes.

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

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

4.2 Such scenarios would include where an accountable institution deems a person or entity to be their client, and this client in turn has their own clients that are not party to the business relationship or single transaction. Such scenarios must be clearly defined as part of the accountable institution's RMCP.

5. COMMUNICATION WITH THE CENTRE

5.1 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.

5.2 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
25 March 2022