



FINANCIAL INTELLIGENCE CENTRE ACT NO. 38 OF 2001 (“FICA”) - INTERNAL POLICY AND PROCEDURES FOR FSP 3425

Introduction

The Financial Intelligence Centre Act, promulgated in 2001 in South Africa and extensively amended in December 2010, sets up anti-money laundering procedures to prevent criminal groups and individuals from converting illegal profits into “clean money”. FICA requires all individuals and institutions to report specified as well as unusual or suspicious transactions to the Financial Intelligence Centre.

The purpose of this Internal Policy and Procedures is to ensure compliance with FICA and to ensure that each employee knows his/her role in complying with the requirements as imposed by FICA.

Training and awareness

Each employee is obliged to read through the FICA training material and receive FICA training. Each employee must ensure that he/she fully understands the contents, duties and obligations in terms of FICA and know how to identify and report a suspicious transaction. After reading the FICA training manual and receiving FICA training each employee must sign and date a training register, which is to be kept on file and updated annually.

Customer acceptance policy

FSPs are expected to develop clear customer acceptance policies and procedures, including a description of the type of customer that is likely to pose a higher than average risk to their business. The FSP takes into account risk indicators, including factors such as the customer's:

- background;
- country of origin;
- public or high profile position; (PEP's)
- linked accounts and;
- business activities

It is the policy of the FSP to accept the following clients as low risk clients:

- Local clients
- Clients transferring monies using EFT and not cash deposits
- Existing clients with whom a relationship is already established
- Clients whereby a relationship is established, and not just a single transaction

Clients not falling into one of the above categories are regarded as high risk. Extensive due diligence for higher risk clients is required. This includes the completion of the risk rate document and obtaining information and verifying the source of income of the client, together with the source of funds.

Identifying the client and verifying the information

All client information required as set out in the FICA act and in the training manual must be obtained from the client with each and every transaction concluded with the company in a diligent and accurate manner. The said information is obtained to ensure that the provider “knows its client” and to ensure the provider knows who it is dealing with. Each document obtained is to reflect the name of the verifier, the date, and what the source document was. Any faxed documents received should only be accepted if the fax was certified prior to its being sent.

Each employee must report transactions concluded by him/her to the reporting officers where the necessary information was not obtainable from the client or where the client refused to disclose or submit the information required.

Unusual or suspicious transactions

Each employee is obliged to report any unusual or suspicious transaction to the reporting officer. Unusual or suspicious transactions are transactions as set out in the training manual or any other transaction concluded by the employee and a client and the employee is not sure whether he knows his client or is unsure of the source of any of the received documents or monies. Each transaction concluded by an employee that seems unusual or suspicious, taking into consideration the experience and qualifications of each employee, must be reported to the reporting officer.

Record keeping

All documents and records relating to each client (“client information”), with whom a transaction was concluded must be maintained and kept in safe custody (protected against destruction) for a period of 5 years from date of conclusion of the transaction or date the relationship with the client was terminated, whichever occurs the latest in time. In this regard all client information must be handed to the money laundering compliance control officer, who can thereafter be contacted to ensure access to client information by employees.

Each employee who removes client information from safekeeping, must sign for such client information and insert the date such client information is removed from safekeeping. On return of such client information the same person who removed such information must sign and date that all client information was returned.

Non-compliance

Each member will be liable to disciplinary action in the event of non-compliance with FICA, the training manual, these Internal Policy and Procedures and all other policies issued from time to time by the company.

Reporting in terms of FICA

Each employee must immediately report a transaction to the reporting officer in the following events:

- a) any cash transaction over the published threshold ; or
- b) any unusual or suspicious transaction; or
- c) when it was impossible for the employee to comply with the requirements in terms of FICA for whatever reason; or
- d) whenever in doubt as to whether to report to the reporting officer or not.

The responsibility to report a transaction in terms of FICA to the Financial Intelligence Centre will transfer from the employee to the reporting officer after a transaction was reported to the reporting officer. The reporting officer will determine and decide as to whether a transaction must be reported.

Reporting officer

The money laundering control compliance and reporting officer for the business is Mrs YE van Esch, or any other person nominated from time to time by the company.

The MLCCO is responsible for regularly checking on the FIC website for legislative updates, plus the issuing of circulars and guidelines.

If the employee has any questions or any queries or is uncertain of any aspect relating to FICA, the employee must report to the reporting officer immediately before any transaction is finalised between the company and a client in order to ensure compliance with FICA.

The reporting officer has to determine within 15 days after the conclusion of any transaction whether or not the transaction is reportable to the Financial Intelligence Centre.

Politically Exposed Persons

A politically exposed person or PEP is the term used for an individual who is or has in the past been entrusted with prominent public functions in a particular country. The principles issued by the Wolfsberg Group of leading international financial institutions give an indication of practice guidance on these issues. These principles are applicable to both domestic and international PEPs.

The following examples serve as aids in defining PEPs:

- Heads of State, Heads of Government and cabinet ministers;
- Influential functionaries in nationalised industries and government administration;
- Senior judges;
- Senior political party functionaries;
- Senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations;
- Members of ruling or royal families;
- Senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities).

According to the Wolfsberg principles, families and closely associated persons of PEPs should also be given special attention by an institution. The term "families" includes close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage. The category of "closely associated persons" includes close business colleagues and personal advisers/consultants to the PEP as well as persons, who obviously benefit significantly from being close to such a person.

An institution should conduct proper due diligence on both a PEP and the persons acting on his or her behalf. Similarly, KYC principles should be applied without exception to PEPs, families of PEPs and closely associated persons to the PEP. This entails obtaining, in addition to the required FICA identification and verification, information and verification of source of income and source of funds.

Treatment of PEPs in relation to other high-risk clients

Specific action should be taken in relation to PEPs as a category of high-risk client. In addition to performing customer due diligence measures, institutions should put in place appropriate risk management systems to determine whether a customer, a potential customer or the beneficial owner is a PEP.

All clients should be asked whether they would fall into one of the categories above, or constitute family of any such persons.

In addition the following is required:

- obtain senior management approval for establishing business relationships with a PEP. When the client has been accepted, the institution should be required to obtain senior management approval to continue the business relationship;
- take reasonable measures to establish the source of wealth and the source of funds of customers and the beneficial owners identified as PEPs;
- conduct enhanced ongoing monitoring of a relationship with a PEP.

Policies for dealing with PEPs:

PEPs should be regarded as high-risk clients and, as a result, enhanced due diligence should be performed on this category of client. Heightened scrutiny has to be applied whenever PEPs or families of PEPs or closely associated persons of the PEP are the contracting parties or the beneficial owners of the assets concerned, or have power of disposal over assets by virtue of a power of attorney or signature authorisation.

The Wolfsberg principles provide additional guidance on how to recognise and deal with a PEP. In addition to the standardised KYC procedures, the following prompts are appropriate to recognise a PEP:

- the question whether clients or other persons involved in the business relationship perform a political function forms part of the standardised process, especially in cases of clients from corruption prone countries;
- client advisers should deal exclusively with clients from a specific country/region to improve their knowledge and understanding of the political situation in that country/region;
- the issue of PEPs should form part of regular KYC training programs;
- may use databases listing names of PEPs including their families, closely associated persons and advisors.

The following questions should be asked at each FICA transaction:

Politically Exposed persons (PEP's)		Yes	No
Is the client one of the following or a close family member or closely associated with one of the following?			
	Heads of state, heads of Government and cabinet ministers		
	Influential functionaries in nationalised industries and Government		
	Senior judges		
	Senior political party functionaries		
	Senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations		
	Members of ruling or royal families		
	Senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities)		

If any questions were answered “Yes”, the source of funds and more information about the transaction and the client should be obtained.

FICA – GENERAL INFORMATION: THIS DOCUMENT MUST ACCOMPANY EVERY FICA TRANSACTION

Client:

Date:

Verifier:

The following questions should be asked at each FICA transaction:

Politically Exposed persons (PEP's)		Yes	No
Is the client one of the following, or a close family member or closely associated with one of the following?			
	Heads of state, heads of Government and cabinet ministers		
	Influential functionaries in nationalised industries and Government		
	Senior judges		
	Senior political party functionaries		
	Senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations		
	Members of ruling or royal families		
	Senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities)		

If any questions were answered “Yes”, the source of funds and more information about the transaction and the client should be obtained.

Source of funds:

Source of income:

Risk rating:

The following factors should be taken into account when risk rating a client and should be implemented at each instance where FICA applies:

		low	med	high
1	Product type – i.e. Complex investments could be high risk and life cover with small savings could be low risk			
2	Business activity			
3	Client attributes, for example, is the client on the United Nations list			
4	Duration of client relationship with FSP – a once off transaction could be high risk			
5	Source of funds; is the source of funds structured e.g. salary (low risk) or cash business (high risk)			
6	Jurisdiction of client; local person (low risk) and foreign national (high risk)			
7	Transaction value; Value less than R..... (low risk) Value between R.....and R.....(medium risk) Value above R.....(high risk)			
8	Type of entity.			