



Financial  
Intelligence Centre

## **PUBLIC COMPLIANCE COMMUNICATION**

**PUBLIC COMPLIANCE COMMUNICATION No 38. (PCC 38)**  
ON THE MODE OF COMMUNICATION REGARDING  
SECTIONS 27, 32, 34 AND 35  
OF THE FINANCIAL INTELLIGENCE CENTRE ACT  
(ACT NO. 38 OF 2001)

**The Financial Intelligence Centre (the Centre) provides the guidance contained in this Public Compliance Communication (PCC) in terms of its statutory function in terms of section 4(c) of the Financial Intelligence Centre Act, 2001, (Act No. 38 of 2001, the FIC Act) read together with Regulation 28 of the Money Laundering and Terrorist Financing Control Regulations (the Regulations) issued in terms of the FIC Act.**

**Section 4(c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations of the FIC Act. Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Regulations issued under the FIC Act. Accordingly, guidance provided by the Centre is authoritative in nature and must be taken into account when interpreting the provisions of the FIC Act or assessing compliance with the obligations it imposes.**

**It is important to note that enforcement action may follow from non-compliance with the FIC Act. Where it is found that an accountable or reporting institution has not followed guidance which the Centre has issued, the institution must be able to demonstrate that it has complied with the relevant obligations under the FIC Act in an equivalent manner nonetheless.**

#### **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**

This PCC is copyright. The material in a PCC may be used and reproduced in an unaltered form only for personal and non-commercial use within your institution. Apart from any use permitted under the Copyright Act No. 98 of 1978, all other rights are reserved.

## **PCC Summary**

**Public Compliance Communication No. 38 (PCC 38) provides guidance to accountable and reporting institutions, and other persons on the mode of communication regarding sections 27, 32, 34 and 35 of the FIC Act.**

## **Objective**

**The objective of this PCC is to provide guidance in relation to receiving and responding to requests, interventions and orders from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act.**

### **1. Application of this PCC**

- 1.1. The Centre has prepared PCC 38 to assist accountable institutions, reporting institutions and any other person to receive and respond to requests for information, interventions and monitoring orders from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act and provides guidance on:
  - How the request will be sent by the Centre;
  - How responses must be submitted to the Centre;
  - The timelines for responses; and
  - Information to be included in the response.
- 1.2. Sections 27, 32, 34 and 35 of the FIC Act provides the Centre with mechanisms to request information in relation to clients, transactions, reports as well as to intervene in certain transactions or proposed transactions.
- 1.3. This PCC should be noted and applied by Heads of Compliance, section 43(b) Compliance Officers, Money Laundering Reporting Officers and persons of similar compliance designations of accountable and reporting institutions, assigned to deal with requests, interventions and orders in terms of sections 27, 32, 34 and 35 of the FIC Act.
- 1.4. This PCC comes into effect from **Tuesday, 02 May 2017**.
- 1.5. PCC38 is divided into 5 parts:
  - Part I practical arrangements applicable to all section 27, 32, 34 and 35 communications
  - Part II deals with section 27 communications
  - Part III deals with section 32 communications

- Part IV deals with section 34 communications
- Part V deals with section 35 communications

## **PART I – Practical arrangements applicable to all section 27, 32, 34 and 35 communications**

### **2. Responsible persons**

- 2.1 Accountable and reporting institutions should as far as possible, have allocated officers to attend to requests, interventions and orders received from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act. .

### **3. Methods of receiving and responding to communications from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act**

- 3.1 The message board on the registration and reporting platform is the main mode of communication from and to the Centre.

- 3.2 In the event that the message board is not functional e.g. due to system maintenance, or if so determined by the Centre, the Centre will utilise encrypted email messages for this purpose, and/or any other secure method as determined by the Centre.

- 3.3 Institutions and persons must respond to instructions in terms of the specified communications sent by the Centre by responding to the original message from the Centre using the same platform through which the instruction was received. Alternatively, the Centre will inform the institution or person which method to use when responding to the Centre.

### **4. Attachments and Reference Numbers**

- 4.1 All relevant and requested information must be attached to the response to requests, interventions and orders from the Centre using the message board, the encrypted email and/or any other secure method as determined by the Centre. Attachments must be in PDF, MS Word and/or in MS Excel format or in a format requested by or agreed to by the Centre.

4.2 The response must contain the relevant reference number, assigned to the relevant response, request or intervention, as provided by the Centre.

## **5. Response times**

5.1 The Centre will specify the required response time for all requests for information interventions and monitoring orders in terms of sections 27, 32, 34 and 35 of the FIC Act.

5.2 All days for calculation of the response times are business days, and exclude Saturdays, Sundays and public holidays.

5.3 Responses must reach the Centre as soon as possible and within the stipulated response time. It is the expectation of the Centre that urgent communications from the Centre be prioritised.

5.4 If the response time cannot be adhered to, the institution or person must contact the Centre using the message board, the encrypted email and/or any other secure method as communicated by the Centre to advise the Centre on the reason for the delay and when the requested information will be provided to the Centre.

## **PART II – Section 27 communications**

### **6. Section 27 of the FIC Act – accountable institutions to advise the Centre of clients**

6.1 Section 27 of the FIC Act is only applicable to accountable institutions.

6.2 Section 27 compels accountable institutions to advise the Centre of its clients in response to a request from an authorised employee from the Centre. The purpose of such requests is to obtain information relating to specified clients of the accountable institution who may be linked to money laundering or terrorist financing activities.

### **7. Examples of practical application**

7.1 The below examples are not exhaustive, they merely demonstrate how to practically apply the guidance given in a particular scenario:

**Example 1:** XYZ Bank receives a request from the Centre in terms of section 27 of the FIC Act to confirm whether Mr A holds an account with XYZ Bank. The request is sent to XYZ Bank using the message board. XYZ Bank responds directly using the message board by replying to the original message sent by the Centre and attaching a response document (in pdf / MS Word / MS Excel etc.), indicating whether Mr X is a client of the XYZ Bank, as well as including any additional information that the Bank can provide. The response contains the relevant reference number, assigned to the case as provided by the Centre.

**Example 2:** The registration and reporting platform is undergoing maintenance, or the message board is not functional. The Centre will not be able to send the section 27 request via the message board. XYZ Bank will then receive a section 27 request for information in terms of the FIC Act from the Centre using an encrypted email message and/or any other secure method as determined by the Centre, to confirm if Mr B holds an account with XYZ Bank. XYZ Bank will respond using email and/or any other secure method as determined by the Centre, replying to the original message as sent by the Centre. This response must contain the relevant reference number, assigned to the case as provided by the Centre. XYZ will then attach a document (pdf / MS word / MS excel etc.) to the response, indicating whether Mr B is a client of the institution or not.

### **PART III – Section 32 communications**

- 8. Section 32 of the FIC Act – reporting procedures and furnishing of additional information**
- 8.1 Section 32 of the FIC Act is applicable to accountable institutions, reporting institutions and any other person that has made a report in terms of section 28 and/or section 29 of the FIC Act.
- 8.2 Section 32 obligates the abovementioned institutions and persons to respond to a request for additional information from the Centre or an investigating authority acting with the permission of the Centre or under the authority of an authorised officer, without delay.

8.3 Requests for information in terms of section 32 of the FIC Act provides the Centre or requesting party with a mechanism to obtain additional information concerning a report submitted, including the grounds for the report.

## 9. Examples of practical application

9.1 The below examples are not exhaustive, and are to be used merely to demonstrate how to practically apply the above guidance given in a particular scenario.

**Example 3:** XYZ Bank receives a request from the Centre for additional information in terms of section 32 of the FIC Act. The request is sent to XYZ Bank using the message board. The Centre requests information to be submitted using the reporting functionality by submitting an additional information file (AIF) or an additional information file transaction (AIFT). XYZ Bank will respond using the AIF and/or AIFT functionality and must also respond to the Centre by replying to the request in the message board. This response must contain the relevant reference number assigned to the case as provided by the Centre. XYZ Bank also attaches a document (pdf / MS word / MS excel etc.) to the response as well as the relevant reference number assigned to the case by the Centre, and the AIF/AIFT reference number/s

**Example 4:** The registration and reporting platform is undergoing maintenance. XYZ Bank receives a request from the Centre for additional information in terms of section 32 of the FIC Act using encrypted email and/or any other secure method as determined by the Centre. XYZ Bank will respond using email and/or any other secure method as determined by the Centre, replying to the original message as sent by the Centre. This response must contain the relevant reference number, assigned to the case as provided by the Centre. XYZ will then attach a document (pdf / MS word / MS excel etc.) to the response, as well as the relevant reference number assigned to the case by the Centre, and the AIF/AIFT reference number/s-

## **PART IV – Section 34 communications**

### **10. Section 34 of the FIC Act – intervention by the Centre**

- 10.1 Section 34 of the FIC Act is applicable to accountable institutions, reporting institutions and any other person required to make a report in terms of section 28, 28A or 29 of the FIC Act.
- 10.2 Section 34 of the FIC Act provides for intervention by the Centre should the Centre, after consulting with the abovementioned institutions or person, have reasonable grounds to suspect that a transaction or a proposed transaction:
- may involve the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities; or
  - may constitute money laundering or a transaction contemplated in section 29(1)(b) of the FIC Act.
- 10.3 The Centre may direct the accountable institution, reporting institution or person in writing not to proceed with a specific action as detailed in the Section 34 request. This can include, but not be limited to not carrying out of a specified transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a prescribed period not exceeding of 5 business days (excluding Saturdays, Sundays and public holidays).

### **11. Examples of practical application**

- 11.1 The below examples are not exhaustive, and are to be used merely to demonstrate how to practically apply the above guidance given in a particular scenario.

**Example 5:** XYZ Bank receives a section 34 intervention that directs the institution not to process any transactions that are linked to an account that may be linked to the proceeds of unlawful activities, for a period of five (5) business days. The directive is sent to XYZ Bank using the message board. Upon receipt of the intervention XYZ Bank responds using the message board. The response includes the reference number, initiation and expiry dates of the directive, and the amount secured.. XYZ Bank will then attach a document (pdf / MS word / MS excel etc.) to the response.



**Example 6:** The registration and reporting platform is undergoing maintenance. XYZ Bank receives a section 34 intervention that directs the institution not to process any transactions that are linked to an account that may be linked to the proceeds of unlawful activities for a period of five (5) business days. The directive is sent to XYZ Bank using encrypted email and/or any other secure method as determined by the Centre. XYZ Bank will respond via email and/or any other secure method as determined by the Centre, replying to the original message as sent by the Centre. The response includes the reference number, initiation and expiry dates of the directive and the amount secured and, the account status and balance to date. XYZ Bank will then attach a document (pdf / MS word / MS excel etc.) to the response.

## **PART V – Section 35 communications**

### **12. Section 35 of the FIC Act – Monitoring Orders**

- 12.1 Section 35 of the FIC Act is only applicable to accountable institutions and relates to monitoring orders granted by a judge designated by the Minister of Justice for the purposes of the Interception and Monitoring Prohibition Act, Act No. 127 of 1992.
- 12.2 The Centre’s function in relation to a monitoring order granted in terms of section 35 of the FIC Act is to make the accountable institution aware of the judicial order issued, to ensure that the accountable institution implements the order and to receive the information to be reported in terms of the order.
- 12.3 Monitoring orders provide the Centre with a mechanism to request the monitoring of all client accounts, including, but not limited to, transactions concluded by a specified person with the accountable institution, or all transactions conducted in respect of a specified account or facility at the accountable institution, if there are reasonable grounds to suspect that:
- Proceeds of unlawful activities or property connected to an offence relating to money laundering or terror financing and related activities, were transferred or may be transferred to the accountable institution;
  - The accountable institution may be used for money laundering purposes or for any transaction contemplated in section 29(1)(b) of the FIC Act;

- The account or other facility has or may receive the proceeds of unlawful activities or property which is connected to an offence relating to terror financing and related activities; or
- The account or other facility is being or may be used for money laundering purposes or for terror financing or related activities or for the purpose of any transaction contemplated in section 29(1)(b) of the FIC Act.

12.4 Type of information that may be required in terms of the order include but are not limited to the following:

- Details of the transactions relating to specified accounts;
- Branch location and time of cash deposits conducted;
- Counter-account details of debits and credits into and from the accounts;
- Street location and time of cash deposits or withdrawals from Automatic Teller Machines (ATMs);
- Copies of account statements;
- Copies of any transactional notifications to and from the client by electronic means including SMS and e-mail messages for online banking purposes; and
- Relevant telephone numbers, e-mail and internet protocol (IP) addresses used to communicate with the client.

### 13. Examples of practical application

13.1 The below examples are not exhaustive, and are to be used merely to demonstrate how to practically apply the above guidance given in a particular scenario.

**Example 7:** XYZ Bank receives a section 35 monitoring order that directs the institution to report transactional information that is linked to an account that may be associated with the proceeds of unlawful activities and or offences related to money laundering. The relevant information must be reported to the Centre on a weekly basis and for an uninterrupted period of three months or any time as may be stipulated in the order. The order is sent to XYZ Bank using the message board. The XYZ Bank will respond using the message board by replying to the original message as sent by the Centre with a reference number relevant to the case the Centre has initiated. XYZ Bank furthermore

attaches all documents (pdf / MS word/ MS excel etc.) that are linked to the transactional information of the monitored account.

**Example 8:** XYZ Bank receives a section 35 monitoring order that directs the institution to report transactional information linked to an account that may be associated with the proceeds of unlawful activities and/or offences related to money laundering. The relevant information must be reported to the Centre on a weekly basis and for three months which will be stipulated in the monitoring order. The order is sent to XYZ Bank using encrypted email and/or any other secure method as determined by the Centre. The XYZ Bank will respond via email and/or any other secure method as determined by the Centre, replying to the original message as sent by the Centre.

## 14. Conclusion

- 14.1 Sections 27, 32, 34 and 35 of the FIC Act provides the Centre with mechanisms to request information in relation to clients, transactions, reports as well as to intervene in certain transactions or proposed transactions.
- 14.2 Accountable and reporting institutions should as far as possible, have allocated officers to attend to requests, interventions and orders received from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act. .
- 14.3 Institutions and persons must respond to communications from the Centre in terms of sections 27, 32, 34 and 35 of the FIC Act, by responding to the original message from the Centre, using the same platform through which the instruction was received. Alternatively, the Centre will inform the institution or person which method to use when responding to the Centre.
- 14.4 The Centre will specify the required response time for all requests for information interventions and monitoring orders in terms of sections 27, 32, 34 and 35 of the FIC Act.
- 14.5 All relevant and requested information must be attached and responses must contain the relevant reference numbers.

Queries on this and other compliance matters can be logged using the web portal on the Centre's website ([click here](#)) or visit [www.fic.gov.za](http://www.fic.gov.za) for alternative contact details.

**Issued By:**  
**THE DIRECTOR**  
**FINANCIAL INTELLIGENCE CENTRE**  
**31 MARCH 2017**

## **SECTION 27 OF THE FIC ACT**

### **Accountable institutions to advise Centre of clients**

If an authorised representative of the Centre requests an accountable institution to advise whether—

- (a) a specified person is or has been a client of the accountable institution;
- (b) a specified person is acting or has acted on behalf of any client of the accountable institution; or
- (c) a client of the accountable institution is acting or has acted for a specified person, the accountable institution must inform the Centre accordingly.

## **SECTION 32 OF THE FIC ACT**

### **Reporting procedures and furnishing of additional information**

(1) A report in terms of section 28, 29 or 31 to the Centre and a report in terms of section 30(1) to a person authorised by the Minister must be made in the prescribed manner.

(2) The Centre, or an investigating authority acting with the permission of the Centre or under the authority of an authorised officer, may request an accountable institution, a reporting institution or any other person that has made a report in terms of section 28, 29 or 31 to furnish the Centre or that investigating authority with such additional information concerning the report and the grounds for the report as the Centre or the investigating authority may reasonably require for the performance by it of its functions.

(3) When an institution or a person referred to in subsection (2) receives a request under that subsection, that institution or person must furnish the Centre without delay with such additional information concerning the report and the grounds for the report as that institution or person may have available.

## **SECTION 34 OF THE FIC ACT**

### **Intervention by Centre**

(1) If the Centre, after consulting an accountable institution, a reporting institution or a person required to make a report in terms of section 28, 28A or 29, has reasonable grounds to suspect that a transaction or a proposed transaction may involve the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities or may constitute money laundering or a transaction contemplated in section 29(1)(b), it may direct the accountable institution, reporting institution or person in writing not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period as may be determined by the Centre, which may not be more than five days, in order to allow the Centre—

- (a) to make the necessary inquiries concerning the transaction; and
- (b) if the Centre deems it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions.

(2) For the purposes of calculating the period of five days in subsection (1), Saturdays, Sundays and proclaimed public holidays must not be taken into account.

(3) Subsection (1) does not apply to the carrying out of a transaction to which the rules of an exchange licensed in terms of the Securities Services Act, 2004 (Act No. 36 of 2004), apply.

## **SECTION 35 OF THE FIC ACT**

### **Monitoring orders**

(1) A judge designated by the Minister of Justice for the purposes of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), may, upon written application by the Centre, order an accountable institution to report to the Centre, on such terms and in such confidential manner as may be specified in the order, all transactions concluded by a specified person with the accountable institution or all transactions conducted in respect of a specified account or facility at the accountable institution, if there are reasonable grounds to suspect that—

- (a) that person has transferred or may transfer the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities to the accountable institution or is using or may use the accountable institution for money laundering purposes or for the purpose of any transaction contemplated in section 29(1)(b); or
  - (b) that account or other facility has received or may receive the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities or is being or may be used for money laundering purposes or for the financing of terrorist or related activities or for the purpose of any transaction contemplated in section 29(1)(b).
- (2) An order in terms of subsection (1) lapses after three months unless extended in terms of subsection (3).
- (3) A judge referred to in subsection (1) may extend an order issued in terms of subsection (1) for further periods not exceeding three months at a time if—
- (a) the reasonable grounds for the suspicion on which the order is based still exist; and
  - (b) the judge is satisfied that the interest of justice is best served by monitoring the person, account or facility referred to in subsection (1) in the manner provided for in this section.
- (4) An application referred to in subsection (1) must be heard and an order must be issued without notice to or hearing the person or persons involved in the suspected money laundering activities.