South African Reserve Bank

Financial Intelligence Centre

NOTICE

Ref: 9/5/1/3

PUBLICATION OF GUIDANCE NOTE 8 ON DIRECTIVE NO. 1 OF 2022 AS ISSUED BY THE SOUTH AFRICAN RESERVE BANK

Thursday, 6 April 2023: The Financial Intelligence Centre (FIC) together with the National Payment System Department (NPSD) of the South African Reserve Bank jointly publish Guidance Note 8.

The Directive 1 of 2022 deals with industry-specific application of the requirements for processing electronic funds transfers as per Recommendation 16 of the Financial Action Task Force (FATF). The Guidance Note 8 provides guidance on the conduct of accountable institutions relating to electronic funds transfer in South Africa, as required in the Directive 1 of 2022. The intention is to align the regimes for combating money laundering and terrorist financing to the FATF Recommendations.

The Directive 1 of 2022 (under draft Directive 3 of 2019) and the draft Guidance Note 102 was made available for comment from Monday, 23 September 2019 with the due date closing at Monday, 14 October 2019. A second round of consultation on draft Guidance Note 102A was commenced on 31 October 2022 and concluded on 18 November 2022.

Following extensive consultation with stakeholders Guidance Note 8 has been updated and released for publication.

For any other queries please contact the FIC's Compliance Contact Centre on 012 641 6000, select option 1, or submit a web query by clicking on: http://www.fic.gov.za/ContactUs/Pages/ComplianceQueries.aspx

Issued by:

The Financial Intelligence Centre

Financial
Intelligence Centre

GUIDANCE NOTE 8

GUIDANCE NOTE 8

ON THE DIRECTIVE FOR CONDUCT WITHIN THE NATIONAL PAYMENT SYSTEM IN RESPECT OF THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS FOR ELECTRONIC FUNDS TRANSFERS (DIRECTIVE 1 OF 2022)

PREFACE

i) The Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act) places obligations on financial institutions and other businesses deemed vulnerable to money laundering and terrorist financing. The Prevention of Organised Crime Act, 1998 (Act 121 of 1998) (the POC Act) introduced the crime of money laundering and provides for the confiscation and forfeiture of the proceeds of crime. The Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) (the POCDATARA Act) introduced measures to address the financing of acts of terrorism.

ii) Compliance with the FIC Act, together with the effective implementation of the POC Act and the POCDATARA Act, contributes to making it more difficult for criminals to hide their illicit proceeds in the formal financial sector and from their criminal activities, and cuts off the resources available to those seeking to use terrorism as a means to promote their cause.

iii) The FIC Act also established the Financial Intelligence Centre (the Centre) which is South Africa's financial intelligence unit, a government entity created to collect, analyse and interpret information disclosed to it and obtained by it. The principle objectives of the Centre are to assist in the identification of the proceeds of unlawful activities, combating of money laundering and the financing of terrorist and related activities and the implementation of resolutions of the United Nations.

iv) In addition, 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 Act. This guidance is published by the Centre in terms of section 4(c) 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 Money Laundering and Terrorist Financing Control Regulations issued under the FIC Act (the MLTFC Regulations). Guidance provided by the Centre is authoritative in nature which means that accountable institutions must take the guidance issued by the Centre into account in respect of their compliance with the relevant provisions of the FIC Act and the MLTFC Regulations. If an accountable institution does not follow the guidance issued by the Centre, it should be able to

demonstrate that it nonetheless achieves an equivalent level of compliance with the relevant provisions. It is important to note, therefore, that enforcement action may emanate as a result of non-compliance with the FIC Act and the MLTFC Regulations where it is found that an accountable institution has not followed the guidance issued by the Centre.

Disclaimer

v) 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 users' legal position. This guidance does not provide legal advice and is not intended to replace the FIC Act or the MLTFC Regulations issued under the FIC Act. The Centre accepts no liability for any loss suffered as a result of reliance on this publication.

Copyright notice

vi) This guidance is copyright. The material in guidance may be used and reproduced in an unaltered form only for non-commercial use. Apart from any use permitted under the Copyright Act (Act 98 of 1978), all other rights are reserved.

GUIDANCE NOTE 8 ON THE DIRECTIVE FOR CONDUCT WITHIN THE NATIONAL PAYMENT SYSTEM IN RESPECT OF THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS FOR ELECTRONIC FUNDS TRANSFERS (DIRECTIVE 1 OF 2022)

Table of Contents

DEFINITIONS

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

"Cover payment" refers to an electronic funds transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

"Directive 1 of 2022" refers to the Directive for conduct within the National Payment System in respect of the Financial Action Task Force recommendations for electronic funds transfers, made in terms of section 43A(2) of the FIC Act as issued by the SARB and published in Government Notice 47019 of 15 July 2022. Reference to "**the Directive"** has the same meaning.

"Electronic funds transfer" as defined in the Directive 1 of 2022, has the same meaning as the term **"wire transfer"** as per FATF recommendation 16 and interpretative notes thereto.

"FATF" refers to the Financial Action Task Force.

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

"Interpretive Notes on Recommendation 16" refers to the additional information provided by the FATF in the interpretation of Recommendation 16. See http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

"MLTFC Regulations" refer to the Money Laundering and Terrorist Financing Control Regulations, 2002, made in terms of section 77 of the FIC Act and published in Government Notice 1595 in Government Gazette 24176 of 20 December 2002, as amended by Government Notice R456 in Government Gazette 27580 of 20 May 2005 and Government Notice R867 in Government Gazette 33596 of 01 October 2010 and

Government Notice 1107 in Government Gazette 33781 of 26 November 2010 and Government notice 1062 in Government Gazette 41154 of 29 September 2017.

"Payment message' is a general term used in this Guidance Note to indicate the prescribed information to flow with the electronic funds transfer as set out in Directive 1 of 2022.

"Recommendation 16" refers to the recommendation regarding wire transfers as issued by the FATF. See http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

"Serial payment" refers to a direct sequential chain of payment where the electronic funds transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks)

Where a term is not defined in this Guidance Note, the definition as provided in the South African Reserve Bank FATF electronic funds transfer Directive 1 of 2022 and FIC Act applies.

1. APPLICATION OF DIRECTIVE 1 OF 2022

1.1. The objective of this guidance note is to provide clarity to accountable institutions on the requirements as set out in the Directive 1 of 2022 as issued by the National Payment System Department (NPSD) of the South African Reserve Bank (SARB), which sets conditions for the processing of electronic funds transfers.

1.2. This guidance note must be read together with the provisions of Directive 1 of 2022.

1.3. Directive 1 of 2022 applies to electronic funds transfers as described in paragraphs 3 of the Directive 1 of 2022, and includes:

1.3.1. Electronic funds transfers where the originator and the beneficiary are separate clients of the same accountable institution; and

1.3.2. Batched electronic funds transfers, including serial payments and cover payments.

1.4. This guidance is applicable to accountable institutions that must comply with the Directive 1 of 2022, either as an ordering financial institution, intermediary financial institution or beneficiary financial institution.

1.5. Although the application of this Directive 1 of 2022 does not have extraterritorial jurisdiction, accountable institutions are reminded that the Directive is applicable to qualifying electronic funds transfers that flow within South Africa, leave South Africa or come into South Africa.

2. THE APPLICATION OF THE GENERAL FIC ACT COMPLIANCE OBLIGATIONS IN THE CONTEXT OF ELECTRONIC FUNDS TRANSFERS

2.1. When implementing the Directive 1 of 2022, accountable institutions are reminded that the Directive is issued through the provisions of the FIC Act. In this context, accountable institutions should consider the Directive 1 of 2022 provisions in their money laundering, terrorist financing and proliferation financing (ML/TF/PF) controls as detailed in their risk management and compliance programme (RMCP). Customer due diligence (CDD)

controls can be mutually applied to both the FIC Act obligations, and the provisions set in Directive 1 of 2022.

2.2 An electronic funds transfer can be either a single transaction or a transaction within a business relationship between the client and the accountable institution, as contemplated in terms of Chapter 3 of the FIC Act and the MLTFC Regulations.

2.3. Before executing an electronic funds transfer, the ordering financial institution, and beneficiary financial institution must have conducted CDD on their respective clients in compliance with the FIC Act and in terms of their RMCP, where applicable. (see Guidance Note 7).

Verifying the accuracy of client information

2.4 "Verify the accuracy" as stated paragraphs 4.8 and 4.9 of Directive 1 of 2022 means that an accountable institution, must verify the required client and the client's associated information being captured in the electronic funds transfer.

2.5 Given that an accountable institution must identify and verify client information prior to concluding a single transaction of R5 000.00 and above, in terms of the FIC Act and read with the accountable institution's RMCP, it is the Centre's view that the information verified in this CDD process, would meet the verification requirements set in Directive 1 of 2022. Information that is not identified and verified as part of the CDD process, would need to be verified through a process as determined by the accountable institution.

2.6 For purposes of Directive 1 of 2022, there would be no need to re-verify CDD information for every transaction made or received by a client, unless there are doubts about veracity of previously obtained information as contemplated in section 21D or where a suspicious transaction report has been submitted to the FIC in terms of section 29 of the FIC Act.

Threshold amount relating to 'verify for accuracy' and related CDD application

2.7. A qualifying electronic funds transfer refers to a cross-border electronic funds transfer that is a single transaction and is above the threshold of R10 000.00 as set out in Directive 1 of 2022.

2.8 Accountable institutions are reminded that the threshold set for CDD requirements in the FIC Act, read with MLTFC Regulation 1A, remains at the amount of R5 000.00. As expressed in paragraph 4.4 of the Directive 1 of 2022, the Directive does not supersede the CDD obligations as set in the FIC Act. As such, the application of CDD processes remains an obligation on clients entering into a single transaction where the amount is R5 000.00 and above.

2.9 Although the Directive 1 of 2022 only requires verification of information for transactions above R10 000.00, an accountable institution in practice, has readily available access to verified client information obtained through their CDD processes. Accountable institutions are therefore strongly encouraged to capture verified information, irrelevant of the value of the transaction, that is accessible to them. This will ensure the accuracy of payment related information in the financial system and will aid the effective access to and use of information by regulators. It is the Centre's understanding that verified information will be available for all transactions above R5 000.00 and transactions concluded within a business relationship, irrelevant of transaction value.

2.10 For a single once-off transaction where the amount is less than R5 000.00 the accountable institution must still obtain and record all the required information as per Directive 1 of 2022 and the FIC Act, although the information would not be subject to verification. Similarly, where this information has been verified, the Centre strongly encourages the verified information to be captured.

2.12 Where a cross-border electronic funds transfer transaction raises suspicion of money laundering or terrorist financing, irrelevant of the transaction amount, the accountable institution is required in terms of the Directive 1 of 2022 to conduct CDD on their client.

2.13 Like with *incoming* cross-border electronic funds transfers read in paragraph 4.9 of the Directive 1 of 2022, where an *outgoing* cross-border electronic funds transfer is a single transaction of less than R10 000.00 to a beneficiary in a high-risk or other monitored jurisdiction by the FATF, an ordering financial institution is strongly urged to verify the accuracy of the originator information as part of effective ML/TF/PF risk mitigation.

Readers should refer to PCC49 for further guidance on ML/TF/PF risks regarding geographies.

Example 1:

Cross-border electronic funds transfer below the R10 000.00 threshold set in Directive 1 of 2022 with no business relationship:

Client X requests that Bank S in South Africa, transfers an amount of R9 900, 00 via an electronic funds transfer to Mr K in Zimbabwe. Client X does not have an arrangement with Bank S for the purpose of concluding transactions on a regular basis. The transaction does not exceed the threshold amount in Directive 1 of 2022 and therefore the requirement to verify the information in the payment message for accuracy does not apply unless the electronic fund transfer is covered in paragraph 4.8 or 4.9 of the Directive (i.e. a suspicious transaction or funds from a high-risk jurisdiction).

Bank S must include the required information in the electronic funds transfer payment message for Client X, in doing so, Bank S has complied with Directive 1 of 2022.

Bank S must conduct CDD on the client in terms of the FIC Act, as the single transaction is more than R5 000.00 as prescribed in terms of regulation 1A of the MLTFC Regulations. Bank S should capture this verified information obtained in the CDD process in the payment message given that it is available to them.

Example 2:

Cross-border electronic funds transfer transaction above the R10 000,00 threshold set in Directive 1 of 2022 with no business relationship

Client Z requests that Bank X in South Africa transfers an amount of R10 001,00 via an electronic funds transfer to Mr J's bank account in Angola.

Client Z does not have an arrangement with Bank X for the purpose of concluding transactions on a regular basis. However, the transaction value exceeds the

threshold set in Directive 1 of 2022 and meets the definition of a single transaction in terms of the FIC Act.

Bank X must therefore verify the information of Client Z in accordance with the requirements as set out in the FIC Act and Bank X's RMCP. Bank X must ensure that the required and accurate information relating to Client Z and required information relating to Mr J as prescribed in Directive 1 of 2022 is included in the cross border electronic funds transfer.

Example 3:

Cross-border electronic funds transfer below the R10 000,00 threshold set in Directive 1 of 2022 and below the CDD verification threshold of R5 000,00 in terms of the FIC Act. No business relationship and a payment from a high-risk country:

Mr P receives an electronic funds payment to the value of R4 900, 00 from Mr O in Syria. Mr P does not have an arrangement with accountable institution F for the purpose of concluding transactions on a regular basis. The transaction does not exceed the threshold amount for a single cross-border payments transaction set in Directive 1 of 2022, nor does it meet the single transaction threshold in terms of the FIC Act, requiring a CDD obligation. However, the electronic fund transfer is processed (coming) from a high-risk country as determined by the accountable institution F.

Therefore, accountable institution F must verify the accuracy of Mr P's information as the beneficiary. The same would apply if there was a suspicion of money laundering and/or terrorist financing.

Example 4:

Cross-border electronic funds transfer transaction below the R10 000,00 threshold set in Directive 1 of 2022 within a business relationship:

Client B in South Africa, makes an electronic funds transfer amounting to R9 900.00 from his bank account at Bank H in South Africa, to Mr T in the Kingdom of Eswatini

on a regular basis. Bank H must ensure that the required and accurate information relating to Client B and required information relating to Mr T as prescribed in Directive 1 of 2022 is included in the cross-border electronic funds transfer. Bank H must conduct CDD on Client B in compliance with the requirements as set out in the FIC Act and its RMCP when establishing a business relationship. It is not required that Bank H re-verifies Client B for each subsequent electronic funds transfer processed, unless part of ongoing monitoring or where Bank H doubts the veracity of information provided by Client B.

2.14 The cross-border electronic funds transfer threshold of R10 000.00 stated in paragraphs 4.7, 4.8 and 4.9 of the Directive 1 of 2022 will be reviewed by the SARB as and when appropriate.

Record keeping of information pertaining to the electronic funds transfer

2.15 The ordering financial institution, intermediary financial institution and beneficiary financial institution must maintain the required information obtained in respect of the originator and beneficiary as prescribed in Directive 1 of 2022 in accordance with the record-keeping requirements in the FIC Act.

3. PRACTICAL APPLICATION OF DIRECTIVE 1 OF 2022 BY ACCOUNTABLE INSTITUTIONS

3.1 Electronic funds transfers effected to or from South Africa and the other Common Monetary Area (CMA) countries, are deemed cross-border electronic funds transfers.

3.2 Where the name of the originator is required, it is the Centre's view that the full names for natural persons, and the registered names for legal persons as captured for CDD of the client should be used.

3.3 Accountable institutions are urged to view PCC 49 to assist in the determination of country (jurisdiction) risk within its risk-based approach. A geographic area that is deemed as presenting a higher ML/TF/PF risk by the accountable institution is considered to be a 'high-risk jurisdiction' as referenced in Directive 1 of 2022.

3.4 An accountable institution must determine its approach of capturing the required information for domestic electronic funds transfers and document this in their RMCPs, for example, whether the accountable institution will be capturing full information in domestic electronic funds transfer messages, or only providing the name of the beneficiary and account number or the unique customer identifier as read with paragraph 4.11 of Directive 1 of 2022.

3.5 In terms of paragraph 4.11 of Directive 1 of 2022, an ordering financial institution must provide the required information referred to in paragraph 4.1 of Directive 1 of 2022 within three business days, to the beneficiary financial institution and to appropriate authorities or supervisory bodies upon request or demand in accordance with any law.

3.6 In turn, the Centre strongly urges accountable institutions to honour all such information requests made to them from other accountable institutions timeously, to allow for the processing of such transactions. Accountable institutions should take note of draft PCC 22A which discusses matters relating to the protection and processing of personal information concerns.

Unique customer identifier

3.7 A unique customer identifier can be used in a domestic and cross-border electronic funds transfer.

3.8 The use of a unique customer identifier for an originator in a cross-border electronic funds transfer must be used with caution, as it may result in the rejection or suspension of transactions due to non-compliance with the international standards of FATF Recommendation 16.

3.9 The use of a unique customer identifier does not apply in respect of the beneficiary. Where proxy resolutions are used by ordering financial institutions, they must ensure that the name and account number of the beneficiary are always carried in the payment message of a domestic electronic funds transfer.

3.10 The use of a unique customer identifier is not considered as a replacement for an identification number. Rather it is to be used as a proxy identifier, that when reviewed

on an accountable institutions' records, they would be able to fully determine the identity of the client as a result of the onboarding and/or CDD obligations.

3.11 A distinction is drawn between the use of a unique customer identifier and a unique transaction reference number. A unique customer identifier refers to the use of a numeric or alphanumeric combination (that denotes the customer address, a national identity number of the client, or a date and place of birth), whereas the unique transaction reference number denotes the identification of an account or transaction number.

3.12 The requirement of 'unique' must be understood in the context of;

3.12.1 The purpose of the identifier is to be used to ascertain the identity of the client held on the entity's records easily, without issue;

3.12.2 The identifier is attributed to only that particular person or client whenever the client engages with the accountable institution at any time;

3.12.3 The identifier is tied to the person or client's identity, and the client or person would not be given a new identifier;

3.12.4 The identifier cannot be recycled or re-assigned to another person or client;

3.12.5 No other person or client has the same number or identifier.

Capturing of an identification number or passport number

3.13 There may be scenarios where the accountable institution holds on record an identification number for a client that is other than a South African identity number or passport number, as obtained during their CDD process for the client.

3.14 An accountable institution may make use of such an identification number where applicable. Such examples would include:

3.14.1 In the instance of a legal person, the entity registration number

3.14.2 Asylum seeker or refugee permit numbers

3.14.3 International bank account number (IBAN).

4. PROCESSING OF INCOMPLETE INFORMATION IN AN ELECTRONIC FUNDS TRANSFER MESSAGE

4.1 Accountable institutions must as part of their RCMPs have clearly documented policies, processes and system controls in place to identify and either execute, reject or suspend electronic funds transfers which do not include the minimum information in the electronic funds transfer message.

4.2 The Centre advises accountable institutions that it would be good practice to develop a system that monitors electronic funds transfer messages, in order to identify electronic fund transfers that do not contain the information as required by Directive 1 of 2022.

4.3 In all instances where an intermediary and/or beneficiary institution has made a determination of how to proceed with an electronic funds transfer transaction that does not contain the required information, the accountable institution must clearly document the decision taken, supported by the rationale for the decision. The Centre recommends that this process be included in the accountable institution's RMCP.

5. PRACTICAL CONSIDERATIONS FOR THE INCLUSION OF INFORMATION IN A QUALIFYING ELECTRONIC FUNDS TRANSFER

5.1 Directive 1 of 2022 does not specify a particular method or mechanism in which information should be captured and included in a qualifying electronic funds transfer.

5.2 The methods or mechanisms used by an accountable institution should take into consideration the particular operational systems and controls of the accountable institution to affect such transfer of information, within the context of the payments systems parameters.

5.3 Examples of such methods or mechanisms that could be considered by an accountable institution may include, but is not limited to;

5.3.1 SWIFT messages

5.3.2 QR code message exchange

5.3.3 Supplementary information files

5.3.4 File message.

6. IMPACT OF DIRECTIVE 1 OF 2022 ON ACCOUNTABLE INSTITUTIONS COMPLIANCE OBLIGATIONS WITH THE FIC ACT

Scrutinising payments and electronic funds transfers to identify sanctions

6.1 The accountable institution (ordering financial institution, intermediary financial institution, and beneficiary financial institution) must scrutinise information obtained in all electronic funds transfers against the sanctions lists as published in terms of section 26A of the FIC Act in order to identify sanctioned persons, regardless of any threshold amount. This is applicable for both cross-border and domestic electronic funds transfers.

6.2 No electronic fund transfers can be processed to or from a person (i.e. originator, or beneficiary) who is designated in terms of section 26A of the FIC Act.

6.3 The accountable institution in possession of the related funds must immediately freeze the funds where a sanctioned person has been identified as party to the payment and must report the fact to the Centre in terms of section 28A of the FIC Act (refer to Guidance Note 6A).

6.4 An accountable institution not in possession of funds must file a terrorist financing transaction or activity report (TFTR/TFAR) in terms of section 29 of the FIC Act.

6.5 It is the Centre's view that for the purposes of traceability and sanctions screening, the name of the beneficiary in all instances should be a name and surname when dealing with a natural person, or a registration name when dealing with a legal person.

6.6 Where a beneficiary name and surname, or a registration name, is not provided in the payment message, the accountable institution should consider whether such exclusion of sufficient information for screening purposes is suspicious and unusual. The use of the term 'unknown' or 'not applicable', numeric characters (incoherent use) or not providing any information for beneficiary information in an electronic funds transfer, where the information is readily available, amounts to a circumvention of South Africa's financial integrity as potentially critical ML/TF/PF information is deliberately held back.

7. COMMUNICATION WITH THE CENTRE

7.1 The Centre has a dedicated compliance contact centre geared to assist accountable institutions to understand their registration obligations in terms of the FIC Act. Should you have any queries please contact the Centre's compliance call centre on 012 641 6000 and select option 1.

7.2 In addition you can submit an online compliance query 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
6 April 2023

Financial Intelligence Centre

CONSULTATION FEEDBACK NOTE AND DETAILED RESPONSES TO COMMENTS RECEIVED

Relating to the draft Guidance Note 102A on the Directive for conduct within the National Payment System in respect of the Financial Action Task Force Recommendations for Electronic funds transfers (Directive 1 of 2022) – Second round of consultation

April 2023

INTRODUCTION

1. The Financial Intelligence Centre (Centre) issued for consultation draft guidance note 102A (draft GN102A) for consideration and the provision of comments on the draft by accountable institutions to the Centre in terms of section 42B of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act) on 31 October 2022, with the consultation period ending on 18 November 2022.

2. Consultation comments were received from banks, financial service providers, industry associations, and consultants.

3. The final version of the draft Guidance Note 102A has been issued as Guidance Note 8.

THEMATIC FEEDBACK

High level feedback on the consultation comments received are noted thematically below:

The difference between the cross-border electronic funds transfer threshold outlined in the Directive and the single transaction threshold in terms of the reference to the Financial Intelligence Centre Act

4. The threshold of R10 000.00 referred to in the Directive 1 of 2022 (Directive) and Guidance Note 8 only refers to the capturing of verified information for cross-border electronic funds transfer.

5. The obligation to conduct customer due diligence (CDD) and all other obligations as stated in the FIC Act continue to apply and have not been replaced by the contents of this Directive. Therefore, all transactions of R5 000.00 and above are subject to CDD obligations as stated in the FIC Act.

6. The Centre strongly urges all accountable institutions to continue to capture validated information, where available, regardless of the value of the transaction.

Applicability of the Directive to specific institutions

7. If the accountable institution initiates or receives domestic and cross-border electronic funds transfers and/or acts as an intermediary in receiving or transmitting

electronic funds transfers, then the Directive and the Guidance is applicable to them. This includes domestic and cross-border electronic funds transfers initiated or processed through payment clearing houses and similar facilities.

8. There are no exclusions to specific accountable institutions performing the activities mentioned in paragraph 7 above.

The applicable threshold as discussed in the Directive is too low

9. The threshold has been increased to R10 000.00 after extensive industry consultation.

The scrutinising of client details in terms of targeted financial sanctions list

10. Accountable institutions are reminded that customers involved in transactions must be scrutinised against the Targeted Financial Sanctions (TFS) list available on the Centre's website. All transactions includes both domestic electronic fund transfers and cross-border electronic funds transfers.

Use of unique identifiers for beneficiaries

11. The Directive allows for the use of unique customer identifier information for originators. Where proxies are used by ordering financial institutions, they must ensure that the name and account number of the beneficiary are always carried in the payment message of a domestic electronic funds transfer.

DETAILED COMMENTS RECEIVED

Comment	Response comments
Commentator A Commentator A believes that this guidance note is not applicable to authorised users as accountable institutions, as all scenarios above are covered in the normal course of business as authorised users who are accountable institutions as named in Schedule 1 of FIC Act. If our understanding and interpretation is correct, we have no further comment. If the FIC takes a different view, we will look forward to receiving you feedback on the matter. We note that all client accounts are CDD'd as required by the FIC Act in line with our documented RMCP's. We do not believe that we are ordering financial institutions, intermediary financial institutions, or beneficiary financial institutions. X therefore is of the view that this guidance note is not applicable to authorised users as accountable institutions, as all scenarios above are covered in the normal course of business as authorised users who are accountable institutions as named in Schedule 1 of FIC Act. If our understanding and interpretation is correct, we have no further comment. Scenario 1 - An authorised user receives transfers from the clients into the Trust accounts. During the settlement, these funds	The definition of the ordering financial institution and the intermediary financial institution: 'ordering financial institution' means an accountable institution that initiates an electronic funds transfer and transfers the associated funds upon receiving the request for an electronic funds transfer from or on behalf of the originator; 'intermediary financial institution' means an accountable institution in a serial or cover payment chain that receives and transmits an electronic funds transfer on behalf of an ordering financial institution and beneficiary financial institution or another intermediary financial institution. The Directive applies to domestic electronic funds transfer transactions and cross-border electronic funds transfer transactions above the threshold and cleared by Payment Clearing Houses (PCH) and similar institutions.

Comment	Response comments
move between institutions and then will be paid to the client based on the transaction concluded i.e., the purchase or sale of a share. Scenario 2 - The authorised user can also be instructed by a client to transfer funds on their behalf and conduct third party payments, in which case the authorised user would have conducted CDD On the client but not on the third party receiving the cash. The assumption is that this CDD obligation would fall onto the receiving parties accountable institution where the account is held. Scenario 3 - The authorised user would also make cross-border payments on behalf of themselves in relation to services provided i.e., Data services, Terminal fees (xx) etc. or for counterparties in relation to the business of an authorised user. We note that all client accounts are CDD'd as required by the FIC Act in line with our documented RMCP's. As such we do not believe that we are ordering financial institutions, intermediary financial institutions, or beneficiary financial institutions.	
2.5 We propose the paragraph to be amended to read - '2.5 It is the Centre's view that the ordering financial institution and the beneficiary financial institution, as accountable institutions, would meet its obligation to verify	Substantial intext amendments have been made. The amendments are to address the use of CDD processes to assist in the verification of information required to be captured, as set out

Comment	Response comments
the accuracy of its client information terms of Directive 1 of 2022, where it has verified its client, per the CDD obligations in terms of the FIC Act and its RMCP.	in the Directive, where such information forms part of the CDD process.
2.6 This implies a transaction by an originator. It is not clear what is intended here, as the originator could make multiple transactions to multiple beneficiaries. See Example 4. Propose the following wording: Delete 'made by a client' For purposes of Directive 1 of 2022, there would be no need to re-verify CDD information for every cross-border transaction, unless there are doubts about veracity of previously obtained information as contemplated in Section 21 D of the FIC Act.	In text amendments made to clarify that re-verification stemming from suspicious transaction reports (STR) or doubts about veracity of information can relate to transactions either made by or received by a client. A suspicion can relate to both the originator and the beneficiary.
2.11 The introduction may cause some confusion. We propose the following amendment – 2.11. Where a cross-border electronic funds transfer transaction raises suspicion of money laundering or terrorist financing, irrelevant of the amount involved, the accountable institution is required in terms of Directive 1 of 2022 to conduct CDD on their client. Deletion of the following: Accountable institutions are reminded that transactions between R5 000,00 and R10 000,00 are subject to CDD requirements as read with paragraph 2.8 regardless of suspicions raised.	All references to the difference in thresholds set in the Directive and the FIC Act (ie. R10 000.00 and R5 000.00) have been redrafted to simply text.

Comment	Response comments
Commentator B 3.3 We propose alignment of 3.3 with 4.9 of the Directive. 3.5. Amend GN wherever it refers to "originating financial institution" to "ordering financial institution". 3.8 We propose the following clause for improved clarity: The use of a unique customer identifier for an originator in a cross-border electronic funds transfer must be used with caution, as it may result in the rejection or suspension of transactions due to non-compliance with the international standards in terms of FATF Recommendation 16.	Reference to jurisdiction, country and geographic area has been considered and updated. Document has been reworded accordingly. Document has been reworded accordingly.
Commentator B The Directive Paragraph 4.6.1 makes the beneficiary name a mandatory field. GN Paragraph 6.6 further defines this field to be name and surname for natural persons and the registered name for legal persons. While we are generally in support of this requirement we highlight at this time certain challenges to the achievement of this, which may require the SARB's support for a period over which market practice is adopted to meet this requirement, especially as it impacts on customers, customer experience, and customer behaviour. The following are current limitations to compliance with this requirement:	These comments have been noted. The integrity of the payment system is reliant on the quality of data that is captured into the system by participants. It is not the expectation that a payments system validate data. Rather, it is the expectation that all participants that capture data into the system validate and perform a level of quality control of data, prior to this entering into the payment system. It is the Centre and the SARB's expectation that accountable institutions drive a

Comment	Response comments
-What information about the beneficiary is known to originating client. Generally speaking the public will know the "trading as" name of legal persons whom they wish to pay, but not the registered name. -What client chooses to input. Furthermore our payment systems are not intelligent enough to determine what is populated in the required in the fields of the EFT, but rather that such fields are populated. -Any field length restriction on the various payment instruction/initiation channels including but not limited to online banking, banking apps, USSD (dial-string), etc. -Any field length restriction on any internal (to bank or sponsored non-bank) messaging/ processing/ data storing systems and -Any field length restriction on the interbank clearing message standard (e.g. EFT180, ISO15001 etc)	behavioural change by urging their customers (in whatever means available to them) to capture quality information regarding the beneficiary.
Commentator C Thresholds seem to be a bit low.	The threshold has been increased to R10 000.00 after consultation with the industry.

CONCLUSION

12. The Centre thanks all commentators and notes that all comments received have been considered and incorporated in Guidance Note 8 where appropriate.

13. The final Guidance Note 8 has been issued on 6 April 2023.

COMMUNICATION WITH THE CENTRE

14. Queries can be directed to the compliance contact centre on 012 641 6000 and select option 1, or 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

Private Bag X177

CENTURION

0046

6 April 2023