GOVERNMENT NOTICE

NATIONAL TREASURY

No. R **2023**

FINANCIAL INTELLIGENCE CENTRE ACT, 2001 (ACT NO. 38 OF 2001): DRAFT AMENDMENTS TO MONEY LAUNDERING AND TERRORIST FINANCING CONTROL REGULATIONS

The Minister of Finance has, in terms of section 77 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), made the regulations set out in the Schedule.

SCHEDULE

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

<u>_____</u> Words underlined with a solid line indicate insertions in existing enactments.

Definitions

1. In these regulations, "the Regulations" mean the Money Laundering and Terrorist Financing Control Regulations, 2002, published in Government Notice No. R. 1595 of 20 December 2002 as amended by GN R456 in Government Gazette 27580 of 20 May 2005, GN R867 in Government Gazette 33596 of 1 October 2010, GN 1107 in Government Gazette 33781 of 26 November 2010, GN R1062 in Government Gazette 41154 of 29 September 2017, GN2638 in Government Gazette 47302 of 14 October 2022 and GN 2943 in Government Gazette 47883 of 20 January 2023.

Insertion of regulation 27E

16. The following regulation is hereby inserted in the Regulations after regulation 27D:

"**Requirements for protection of personal information in respect of sharing of information between accountable institutions**

27E. (1) For the purposes of carrying out the provisions of section 29 as contemplated in section 41A(3) of the Act, an accountable institution must

ensure the integrity and confidentiality of the personal information of the client of the accountable institution by taking appropriate, reasonable and organisational measures when sharing information to another accountable institution to prevent—

(a) alteration or loss of, damage to or unauthorised destruction of the information; and

(b) unlawful access to or further processing of the information, other than in accordance with the Act and the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

(2) In order to appropriately secure the integrity and confidentiality of the personal information contemplated in subregulation (1) an accountable institution must—

(a) identify all reasonably foreseeable internal and external risks related to the transmission of the information;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to the new risks or deficiencies in previously implemented safeguards.

(3) An accountable institution must comply with the requirements relating to disclosure contained in section 29 of the Act when sharing information relating to a client as contemplated in section 41A(3) of the Act.

(4) The sharing of information of a client may only occur in accordance with a written agreement between the accountable institutions that regulates the exchange of information.

(5) The accountable institution must notify the Centre of—

(a) the name of the receiving accountable institution;

(b) the identifying particulars of the client; and

(c) the date the information was shared,

when it shares information in terms of this regulation.

(6) The notification referred to in subregulation (5) must be made as soon as reasonably possible but no later than five days after the date on which the information was shared.

(7) If there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person, the receiving accountable institution must notify—

(a) the Centre; and

(b) the accountable institution that shared the information.

(8) The notification referred to in subregulation (7) must be made as soon as reasonably possible but no later than five days after the discovery of the compromise.

(9) The notification referred to in subregulations (5) and (7) must be made in accordance with the format specified by the Centre, and sent to the Centre electronically by means of—

(a) the internet-based reporting portal provided by the Centre for this purpose at the following internet address: http://www.fic.gov.za ; or

(b) a method developed by the Centre for this purpose and made available to a person who is required to provide the notification in question.

(10) An accountable institution must keep a record, as the case may be, of—

(a) the information that the accountable institution shares in accordance with this regulation;

(b) the information that the accountable receives in accordance with this regulation; and

(c) the purpose for the request.".

Amendment of regulation 29

2. Regulation 29 of the Regulations is hereby amended by the insertion after subregulation (7) of the following subregulation:

"(7A) Any person or institution who—

(a) fails to act in accordance with regulation 27E in respect of the sharing of information of a client; or

(b) fails to notify the Centre as required by regulation 27E,

is non-compliant and is subject to an administrative sanction.".

Commencement

3. The Regulations take effect on xxxxx.

EXPLANATORY MEMORANDUM

1. INTRODUCTION

1.1 Those involved in money laundering and other financial crimes usually do not just target one business. Frequently they deliberately open and maintain many accounts at different institutions. Without information sharing, it is difficult for accountable institutions to recognize whether transactions are part of an economic crime because institutions cannot connect their customers' transactions within the overall pattern of transactions at other institutions to know if any suspicious activity is occurring.

1.2 Therefore, the ability to share information is critical to identifying, reporting, and preventing financial crime.

2. DISCUSSION

2.1 The Financial Intelligence Centre (FIC) was established in terms of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001, the FIC Act) to assist in the identification of the proceeds of unlawful activities, the identification of persons involved in money laundering activities, offences relating to the financing of terrorist and related activities and proliferation financing activities, and the combating of money laundering activities and, the financing of terrorist and related activities and proliferation financing activities, among others. A key capability for the FIC in achieving this objective is to "follow the money". This means that it is of paramount importance to the success of the FIC's work that it should be able to generate a view of how funds move from one person or institution to another.

2.2 The information that the FIC has at its disposal to reconstruct financial flows when it follows the money comprises mainly of information contained in reports that accountable institutions make in terms of the requirements of the FIC Act. However, when an institution processes a transaction, it sees only one side of it. The information that it is able to report to the FIC in respect of that transaction is therefore, by nature, only one piece of a puzzle. This puzzle may turn out to be a large and complex web of transactions, involving any number of counterpart institutions, when viewed holistically. Criminals, terrorist organisations and

proliferators of weapons of mass destruction exploit this inefficiency in the reporting system to raise, use and move illicit funds in our financial system, while staying ahead of the efforts of the FIC and law enforcement agencies to follow the money.

2.3 The FIC believes that developing further enhancements to information-sharing can help accountable institutions to understand the full picture relating to scenarios that may lead to reporting suspicious or unusual transactions or activities to the FIC. Such enhancements relate to bringing information from different sources together in responsible ways through information-sharing arrangements between accountable institutions.

2.4 However, the sharing of customers' identity and transaction information between accountable institutions raise policy and operational considerations and trigger privacy concerns. The Financial Action Task Force (FATF) recently adopted a report with observations and lessons learnt from countries that have established initiatives for private sector information sharing.[1] This report highlights issues that countries should consider when embarking on establishing a private sector information-sharing mechanism and provides examples of how countries have addressed these. The report emphasises the role of competent authorities in providing regulatory clarity on the policy stance relating to private sector information-sharing. This report provides a useful reference for the FIC's views on private sector information-sharing.

3. DRAFT REGULATIONS RELATING TO THE SHARING OF INFORMATION BETWEEN ACCOUNTABLE INSTITUTIONS

3.1 Section 41A(3) to the FIC Act was amended by the General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022. This provision empowers the Minister of Finance to make regulations that will facilitate the sharing of information between accountable institutions when the sharing of information is necessary for the purposes of carrying out the provisions of section 29.

[1] FATF report: PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME - DATA PROTECTION, TECHNOLOGY AND PRIVATE SECTOR INFORMATION SHARING, published in July 2022.

3.2 These draft regulations give effect to section 41A(3) of the FIC Act and an explanation of the requirements set out in the draft regulations are provided in the paragraphs below.

Sharing of information to be in accordance with the FIC Act and Protection of Personal Information Act, 2013

3.3 The sharing of the content of reports about suspicious or unusual transactions or activities, or about the fact that such a report was made, must be treated with the utmost circumspection. The prohibitions of section 29(3) and (4) also apply in this scenario. However, the consequences of information about a report under section 29 inadvertently coming to the attention of the subject of such a report can be much more detrimental to an investigation that may flow from such a report.

3.4 The principles relating to the protection of personal information as set out in the Protection of Personal Information Act, 2013 (the POPI Act) must be adhered to at all times when customers' personal information is shared in terms of the regulations. These principles are therefore not optional and institutions would not be able to claim compliance with the reporting obligations of the FIC Act, as justification for failing to adhere to any principles contained in the POPI Act.

Ensuring integrity and confidentiality of personal information

3.5 The sharing of customer data introduces possibilities for persons to exploit security vulnerabilities and access the relevant information without the requisite authority to do so. This makes the protection of the security of shared customer data an important consideration in any construct to share customer information between accountable institutions.

3.6 Against this background, accountable institutions that participate in information sharing arrangements would need to devise a platform where they can engage and exchange information. This is a fundamental step as any leakage of shared customer data coming out of an information sharing arrangement could have serious consequences undermining public trust in the institutions involved, not to mention the harm for the individuals involved.

3.7 Advancements in technology such as encryption of communication and the pseudonymisation of data offer some protection that may be considered in this context. Accountable institutions should therefore give serious consideration to

the use of these and other technologies when they develop the infrastructure that they will use to pool and share customer information.

Sharing of information may only be in accordance with written agreement

3.8 When accountable institutions enter into information-sharing arrangements, it is important that they agree on the scope of the customer information that will be shared between them. This is particularly relevant when the sharing of customer information takes place at a stage when an accountable institution is in the process of forming a suspicion. It is important for all the participants in an information-sharing arrangement to understand and share the same expectation as to the limitations on the extent to which customer information is to be shared to aid them in understanding suspicious transactions that take place across different institutions.

3.9 In the same vein, participants in an information-sharing arrangement should be in a position to provide each other with reasonable assurances of the reliability of the customer information that they will share with each other. In addition to a shared expectation as to the scope of customer information that will be shared, having a common view of the accuracy of that information, will contribute to the effectiveness of an information-sharing arrangement. In a worst case scenario, sharing of unreliable or insufficiently verified customer information, can lead to "false positive" reporting of suspicious or unusual transactions, or to the masking of suspicions that should be reported.

Accountable institution to notify the FIC and keep a record when it shares information

3.10 The FIC Act does not require that accountable institutions obtain the FIC's permission to share customer information with each other. However, given the sensitivity of the information that is likely to be shared between accountable institutions when one or more of them is contemplating the reporting of a suspicion to the FIC, and the impact that such a sharing of information may have on the FIC's operations, it is important that the FIC be made aware of any initiative between accountable institutions to share information in this context.

3.11 It is against this background that the draft regulations provide that an accountable institution that shares personal information for the purposes of reporting under section 29 of the FIC Act, must notify the FIC as soon as possible of that sharing

of information. The FIC has developed a dedicated portal on its electronic platform for the reporting of suspicious or unusual transactions, which accountable institutions must use to advise the FIC of the sharing of information in this context.

3.12 Once the FIC is made aware that an accountable institution is sharing personal information with another institution for the purposes of reporting under section 29 of the FIC Act, it will work with the relevant institutions to facilitate the making of such a report. However, the decisions as to the making of the report and coordination between the relevant institutions in this regard, remains the responsibility of the institutions that are involved in the information-sharing arrangement. Proper coordination will avoid the situation of one institution presuming that the responsibility to report in terms of section 29 is that of the other institution and fails to make a report to the FIC.

3.13 It is also important for accountable institutions to keep a record of the information that the accountable institution shares in accordance with this regulation. The register of information shared will assist in the supervision for compliance with the provisions of the FIC Act and regulations with regards to the sharing of information.

De-risking and defensive reporting

3.14 The sharing of information that may be relevant to a report under section 29 of the FIC Act between accountable institutions is likely to bring information about an institution's client to that institution's attention, which may require the institution to re-assess the money laundering and terrorist financing risks relating to the relationship with that client. In doing so an accountable institution should apply its normal risk assessment processes and consider the additional information about its client in the context of all the information at its disposal that may be relevant to its classification of the money laundering, terrorist financing and proliferation financing risks pertaining to its relationship with that client.

3.15 Overreliance on information about potentially suspicious behaviour of a client that is shared by another institution could potentially lead to a situation where an accountable institution would base a decision to limit or deny a client's access to the institution's products and services, solely on third party information, which may be inaccurate.

3.16 The FIC believes that accountable institutions should avoid situations where the sharing of information in the context of reporting under section 29 of the FIC Act leads to the termination of business relationships with clients or the limitation or denial of services to clients. Apart from the policy considerations relating to inappropriate de-risking, a decision of an accountable institution to deny or limit the services provided to a client may also have negative operational consequences if it interferes with the FIC's ability to monitor a person's financial activity through continued reporting under the FIC Act.

3.17 Since the purpose of an information-sharing arrangement is to identify suspicious conduct across multiple accountable institutions, it naturally leverages information from more than one institution. This places an institution in a position where it becomes aware that another institution has filed, or is contemplating the filing of, a suspicious or unusual transaction report that implicates its customer. This has the possibility of exacerbating defensive reporting of suspicious or unusual transactions.

3.18 The mere existence of a suspicion in one institution does not, in and of itself, necessitate the systematic reporting of the same suspicion by another institution that receives such information. However, the shared information may be an important element of an institution's own analysis, which may result in increased instances of identified suspicions. This may provide opportunities for accountable institutions to coordinate the filing of suspicious or unusual transaction reports. However, these arrangements need to be clearly understood and agreed between institutions that participate in an information-sharing arrangement.