Effective date: 28 October 2022

GUIDELINES FOR FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS GUIDELINES NO. FIU/G-2/2022/2

GUIDELINES ON THE OBLIGATION TO SUBMIT A SUSPICIOUS TRANSACTION REPORT (STR) UNDER SECTION 15 OF THE CRIMINAL ASSET RECOVERY ORDER, 2012 AND SECTION 47 OF THE ANTI-TERRORISM ORDER, 2011

1. INTRODUCTION

1.1. These Guidelines are made pursuant to section 15 (6) of the Criminal Asset Recovery Order (CARO), 2012 and section 47 (5) of the Anti-Terrorism Order (ATO), 2011.

1.2. These Guidelines provide guidance to all Financial Institutions and Designated Non-Financial Businesses and Professions (FIs and DNFBPs) on the obligation to report suspicious transactions as required under section 15 of CARO and section 47 of ATO.

1.3. FIs and DNFBPs play a vital role in reporting any transaction or any attempted transaction that is suspected to be related to any serious offence[1] or money laundering offence including terrorist financing[2] to the Financial Intelligence Unit (FIU), Brunei Darussalam Central Bank.

1.4. Suspicious transaction reporting is part of the Financial Action Task Force (FATF) 40 Recommendations, the international standard on anti-money laundering and combatting the financing of terrorism. Compliance with the FATF 40 Recommendation reflects the country's ability to combat money laundering and terrorism financing.

1.5. These Guidelines shall take immediate effect.

2. PURPOSE

2.1. These guidelines have the following objectives:

2.1.1. To assist FIs and DNFBPs in understanding and implementing the requirement to comply with suspicious transaction reporting obligations; and

2.1.2. To assist FIs and DNFBPs to identify suspicious transactions by providing indicators.

3. WHO ARE REQUIRED TO SUBMIT STRs?

3.1. FIs and DNFBPs as defined in Part I, section 2 of CARO and ATO are required to submit Suspicious Transaction Reports (STRs).

4. WHAT ARE SUSPICIOUS TRANSACTIONS?

4.1. Suspicious transactions are those transactions that have occurred including attempted transactions that you suspect or have reasonable grounds to suspect are related to any serious offence, including money laundering and terrorist financing. There is no monetary

[1] Serious offence has the same meaning as section 2 of CARO.

[2] Terrorism financing offence has the same meaning as section 2 CARO/ATO.

or other threshold for reporting STRs, i.e., all suspicion should be reported, regardless of value.

4.2. As a general rule, a suspicious transaction will often be one which is inconsistent with a customer's known employment, profession, legitimate business or personal activities or with the normal business for that type of customer. Identification of suspicious transactions should prompt further enquiries and where necessary, investigations into the source of funds. However, care should be taken to not alert the customer (see section 6 – Tipping Off).

4.3. To enable easier identification of inconsistent activity or behavior, it is encouraged to undertake the following actions:

4.3.1. Ensure customer profiles are established and updated, including obtaining records containing basic identification information, employment, other source of funds, nature of business/use of any particular account, etc.[3]; and

4.3.2. Conduct transaction monitoring via an appropriate system or manually depending on the volume and/or sophistication of transactions conducted.

4.4. Where the customer profile is established and up to date, it becomes easier to detect any irregularities or unusual activities conducted by a particular customer that may be just cause to trigger an STR.

4.5. In most cases, it may not be possible to identify the actual criminal activity that is occurring. To assist in detecting suspicious transaction, FIs and DNFBPs may refer to or screen transactions against red flag indicators, typologies and case studies. Please refer to a list of red flag indicators provided in **Appendix 1**. Sometimes it may require a combination of the indicators to occur for it to be suspicious and ultimately the question of reasonable grounds for suspicion of a serious offence is one that will require an element of human judgement.

4.6. Where a criminal offence can be identified such as fraud, forgery and corruption, it is advisable to report such cases directly to the relevant law enforcement agencies. However, such cases should also be reported as STRs at the same time as a report is made to any law enforcement agencies. This will enable the identification of trends, understanding of different predicate offences detected and captured by the FIs and DNFBPs which can be used to enhance assistance by FIU to law enforcement agencies and feedback to the FIs and DNFBPs.

4.7. The obligation to report an STR also applies when there is a simple suspicion that funds are the proceeds of a criminal activity, regardless of any other transaction or attempted transaction.

[3] This should, in any event, be collected and updated as part of customer due diligence measures

5. WHEN TO REPORT SUSPICIOUS TRANSACTIONS

5.1. All STRs should be submitted to the FIU immediately and as soon as possible, **no later than 3 working days** after a suspicion has been established. Suspicion can be established upon verification of findings and/or further analysis conducted by the compliance officer.

5.2. Any terrorism-related STR should be reported **less than 24 hours** after suspicion or reasonable grounds for suspicion is established, to allow prompt action by the relevant authorities.

5.3. The process leading up to the submission of an STR can be described as follows:

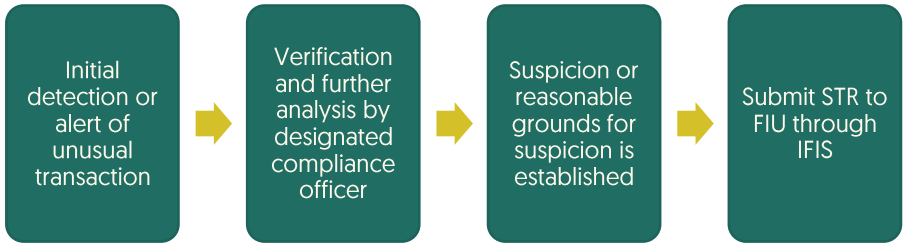
5.3.1. **Initial detection or alert of unusual transaction** – this can be from the frontliners or during monitoring of accounts;

5.3.2. **Verification and further analysis by designated compliance officer** – this stage involves the FIs and DNFBPs gathering and verifying information of the customer and transaction(s) to determine if the transaction is suspicious or if there is reasonable ground to suspect the transaction is linked to criminal proceeds or terrorism financing. FIs and DNFBPs should demonstrate the time taken for this stage is effective and reasonable, avoiding unnecessary delay and support timely submission of STR to the FIU;

5.3.3. **Suspicion or reasonable grounds for suspicion are established** – the moment the compliance officer establishes suspicion or reasonable grounds to suspect the funds are linked to criminal proceeds or terrorism financing; and

5.3.4. **Submit STR to FIU through the Integrated Financial Intelligence System (IFIS)** – Compliance officer will then complete an online form on IFIS website.

Different stages leading up to the submission of an STR to the FIU:



5.4. After an STR has been filed, FIs and DNFBPs may continue the relationship with customer. However, any repeated transaction or continuing pattern of activity in the next quarter or 3 months after, that is still considered suspicious, should be reported again to the FIU to indicate that the suspicious activity is still ongoing.

5.5. Should your institution decide to cease any business relations with that customer, this action should be reported to the FIU, prior to notifying the customer. Notification of such action to the FIU should be included in the STR or through the secured message board in IFIS, if the decision was made after STR was submitted.

Note: There is no requirement for institutions to exit the relationship or stop dealing with the customer when you have reported or are preparing to report STRs. This is entirely up to the institution and your business practices. However, care should be taken not to alert the customer (see section 6 – Tipping Off).

6. TIPPING OFF

6.1. Confidentiality of STR information is crucial in protecting the interest and security of the FIs and DNFBPs, the compliance officers, the FIU and the public. STR information contains private and sensitive financial information as well as unproven allegations relating to individuals and entities. Breaches of confidentiality may undermine the suspicious transaction reporting system and any prevention or enforcement against criminal activities that could have been resulted from the STR.

6.2. Tipping off is one of the several measures provided by CARO to protect the confidentiality of STRs. Once an STR is submitted to the FIU, FIs or DNFBPs (including directors, partners, officers, principals or employees) are prohibited to disclose, share or inform to the customer(s) or any third party in any way or form (either through verbal, printed or electronic means) that an STR has been lodged or that an investigation is being or has been carried out on them.

6.3. FIs and DNFBPs should take reasonable measures in ensuring confidentiality of STR information by limiting the number of employees that have access to STRs or any information that would enable the subject of an STR be identified.

6.4. For FIs or DNFBPs that are a branch or subsidiary with their compliance function located at the overseas head office, the branch management should ensure that sufficient measures are in place for the compliance function to carry out its obligations on reporting of suspicious transactions. In fulfilling obligations to file an STR, this would include the sharing of private and sensitive information contained within an STR. For any private or sensitive information that is shared by the branch in Brunei Darussalam, only those authorized by the compliance officer should have access to such information.

6.5. Important: If fulfilling the customer due diligence could result in tipping off, FIs and DNFBPs **should not** proceed with the due diligence process and immediately submit an STR as stated in section 11 of CARO.

6.6. You should not be requesting information from the individual conducting or attempting the transaction that you would not normally request during a transaction or during the business relationship.

7. HOW TO REPORT AN STR

7.1. STRs are to be submitted online through the IFIS website (https://ifis.bdcb.gov.bn) using one of the following methods:

7.1.1. **Completing an online form**: Compliance officers can complete an STR form by filling in information about the suspicious transactions manually on the IFIS website.

Technical requirements are included in the Reporting Instructions document that are provided upon registration to IFIS;

7.1.2. **Uploading XML files**: STR information can be uploaded in bulk/batch via the IFIS website. This option allows extracting the suspicious transaction information directly from your database and submit automatically to IFIS by converting the information into an XML format. A limit of 5MB is set for each upload.

XML Script which specifies the necessary fields (mandatory & optional) for this option is available upon request from the FIU to all FIs and DNFBPs.

7.2. All FIs and DNFBPs should be registered with IFIS. If your institution is not yet registered, please contact IFIS helpdesk at 2382614 or email at ifishelpdesk@bdcb.gov.bn.

8. WHAT TO INCLUDE IN AN STR

8.1. At the basic level, an STR should cover the basic questions of Who, What, Where, When, How and Why. An ideal STR should include as much information known of the persons/entities involved and the suspicious transaction. Relevant and updated documents should be attached to support arguments for suspicion.

8.2. The technical information below should be present in submitting an STR:

8.2.1. Identification information such as:

(a) For individuals – Full name, identity card number, etc;

(b) For corporations – Full name, date and place of incorporation and if possible, details of beneficial owners/directors and shareholders;

8.2.2. Transaction details including amount involved, type of transactions (wire transfer, withdrawal, attempted, etc), source and beneficiary of transaction and date of transactions;

8.2.3. Description of the suspicious transaction including why it is suspicious. Please include diagrams if necessary to facilitate description;

8.2.4. If there is no actual transaction, details of the facts that give rise to the suspicion;

8.2.5. Action taken or that will be taken with regards to the account/ transaction such as account under monitoring, ordered to close, reject transactions or will exit relationship in 3 months; and

8.2.6. Latest customer profile such as account opening document on each person/entity with updated information should be attached as supporting document.

8.3. The below is a guide to what to include in an STR description or narrative:

8.3.1. **Who** is involved: In addition to providing identification information in the appropriate fields in an STR, it is advisable that a brief background of the individuals or entity involved also be included in the description;

Example: Mr X is a 45-year-old business man who works at Company A as a Supervisor. He receives a monthly salary of $X a month and also receives approximately $Y a month which he claims are proceeds from real estate rental fees.

8.3.2. **What** activity is occurring: In addition to any transaction input in the STR, the narrative should point out what kind of transactional or other activity occurred or was attempted as well as any other transactions if there were not input to the transaction section of the report. It is also helpful to include information on the behaviour of the customer (e.g. If they were uncooperative), and actions by the teller, relationship manager or any officer that was involved over the course of establishing suspicion;

8.3.3. **When** the activity is occurring: Timeline (preferably in chronological order) is important so the date of transactions or other activity occurring should be included in the narrative;

Example: The relationship manager called the customer on X day of X month of X year in order to ask for additional information on their transaction conducted on X day of X month of X year.

8.3.4. **Where** the activity is occurring: There should be an indication of where the activity is occurring e.g. At X district or X branch;

8.3.5. **How** the activity is occurring: Indicate whether the activity occurred face-to-face (e.g. over the counter) or non-face-to-face (eg. ATM/CDM), through electronic means (e.g. Email, fax, internet) or other means (e.g. over the phone); and

8.3.6. **Why** the bank has considered the transaction, attempted transaction or other behaviour linked to funds as suspicious, including:

(a) Indication of a serious offence, if apparent e.g., The customer is involved in fraudulent activity as he is using falsified documents to conduct purchases etc.; and/or

(b) Red flag indicators or triggers observed by your institution.

8.4. It is important that FIs and DNFBPs fulfill the basic information required in the STR form. Sufficient information can assist the FIU in understanding the background for analysis and for law enforcement agencies to investigate. The information required for each STR will vary according to each report but sufficient information must be provided in all cases.

9. WHAT HAPPENS AFTER AN STR IS RECEIVED BY FIU?

9.1. STRs received from FIs and DNFBPs are analysed to determine if activities conducted by the reported individuals/entities involved are suspicious or are linked to any suspicious activity or any existing investigation. The FIU gathers additional information from government and non-government databases and in some cases from foreign counterparts in its analysis process.

9.2. If, after analysis and additional information gathering is conducted, the FIU finds enough information to substantiate a link between the activities to a serious offence, the information will be disseminated to the relevant law enforcement agencies for investigation. Otherwise, STRs are stored in the FIU's database for future reference and may be used to support any future analysis.

10. FEEDBACK

10.1. The FIU may provide the following feedback:

10.1.1. Quality of STRs submitted

As part of ongoing improvement in the quality of STRs submitted, the FIU will provide feedback in terms of missing important details, description of suspicious activities, etc. This will assist FIs and DNFBPs in reporting future suspicious activity and a better understanding of a good STR. Generally, the better quality of an STR, the more it will assist in better understanding/faster analysis and action on the suspicious activity.

10.1.2. Trends and typologies

The FIU will provide feedback of common indicators or current trends and typologies observed from the STRs received from different FIs and DNFBPs. This

aims to facilitate awareness of current activities that may not be detected in your institution, that you should be vigilant of when monitoring transactions conducted in your institution.

10.1.3. If STR has led to successful investigation

It is always good to know if what has been reported as a STR has resulted in the detection and prevention or the successful conviction of a criminal activity. As you may be aware, information with regards to any open investigation cannot be revealed as such updates can only be provided after conviction in court. Note that the lack of information on successful investigations should not be taken as an indicator of the usefulness of an STR.

11. HOW TO CONTACT THE FIU

11.1. These Guidelines will be reviewed on a periodic basis. If you have any comments or suggestions to help improve this paper, or for further information on STR submission, please contact the FIU:

Address	Financial Intelligence Unit Brunei Darussalam Central Bank Level 7, Ministry of Finance and Economy Building Commonwealth Drive Bandar Seri Begawan BB 3910 Brunei Darussalam
E-mail Address	fiu@bdcb.gov.bn
Telephone No.	+673 238 2614

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 2 Rabiulakhir 1444H / 28 October 2022M