FINANCIAL INTELLIGENCE UNIT
AUTORITI MONETARI BRUNEI DARUSSALAM

GUIDANCE PAPER TO FINANCIAL INSTITUTIONS
FOR THE OBLIGATION TO SUBMIT A SUSPICIOUS TRANSACTION REPORT (STR) UNDER
SECTION 15 OF CRIMINAL ASSET RECOVERY ORDER AND SECTION 47 OF ANTI-TERRORISM ORDER

1. Introduction

These Guidelines provide guidance to all financial institutions on the obligation to report suspicious transactions required under Section 15 of the Criminal Asset Recovery Order, 2012 (CARO) and Section 47 of the Anti-Terrorism Order, 2011 (ATO). This guideline is issued pursuant to Section 15 (6) of CARO that allows Autoriti Monetari Brunei Darussalam to issue directions or guidelines on the procedures for and from which the reports shall be submitted and shall publish guidelines in order to assist financial institutions to fulfill their obligations under this section.

These Guidelines should be read in conjunction with these Sections:

> **SECTION 15 (1), CARO: OBLIGATION TO REPORT SUSPICIOUS TRANSACTIONS**
> Subject to subsection (2), financial institutions, designated non-financial businesses and professions, and their respective directors, principals, officers, partners, professionals and employees, that suspect or have reasonable grounds to suspect that a transaction or attempted transaction involving property is related or linked to a serious offence or a money laundering offence shall submit promptly after forming a suspicion a report setting forth the suspicions to the Financial Intelligence Unit.

> **SECTION 47 (1), ATO: OBLIGATION OF FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS TO REPORT SUSPICIOUS TRANSACTIONS**
> Subject to subsection (2), financial institutions, designated non-financial businesses and professions, and their respective directors, principals, officers, partners, professionals and employees, that suspect or have reasonable grounds to suspect that a transaction involving property is related or linked to, or is to be used for, terrorism, terrorist acts, terrorists or terrorist groups or those who finance terrorism shall submit promptly after forming a suspicion a report setting forth the suspicions to the Financial Intelligence Unit. This obligation shall also apply to attempted transactions.

Financial institutions play a vital role in reporting any transaction or attempted transaction that is suspected to be related to any criminal offence including money laundering and terrorist financing, to the Financial Intelligence Unit (FIU), Autoriti Monetari Brunei Darussalam.

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. Ability to comply with the FATF 40 Recommendation reflects the country's ability to combat money laundering and terrorism financing.

2. Purpose

This guideline has the following objectives:-

- To assist reporting entities in understanding the requirement to comply with Suspicious Transaction Reporting (STR) obligations
- To assist reporting entities to identify suspicious transactions by providing indicators

3. Who is required to submit a Suspicious Transaction Report?

Financial Institutions are defined in Part I, Section 2 of CARO and ATO:

FINANCIAL INSTITUTION means –

a) in relation to Brunei Darussalam –

i. a bank licensed under section 4 or 23 of the Banking Order, 2006 (S 45/2006), an international bank licensed under section 7 of the International Banking Order, 2000 (S 53/2000) and an Islamic bank licensed under section 4 or 23 of the Islamic Banking Order, 2008 (S 96/2008);

ii. the Perbadanan Tabung Amanah Islam Brunei established by section 3(1) of the Perbadanan Tabung Amanah Islam Brunei Act (Chapter 163);

iii. any insurer registered under the Insurance Order, 2006 (S 48/2006) or the Takaful Order, 2008 (S 100/2008) or any person licensed under the International Insurance and Takaful Order, 2002 (S 43/2002);

iv. any finance company licensed under the Finance Companies Act (Chapter 89);

v. any person licensed under the Mutual Funds Order, 2001 (S 18/2001), the Securities Order, 2001 (S 31/2001) or the International Insurance and Takaful Order, 2002 (S 43/2002);

vi. any person licensed to carry on any money-changing business or remittance business under the Money-Changing and Remittance Businesses Act (Chapter 174); or

vii. such other person licensed, approved or regulated by the Authority under any written law.

b) in relation to any country outside Brunei Darussalam, a person lawfully carrying on therein business corresponding in whole or in part to banking business as defined in section 2(1) of the Banking Order, 2006 (S 45/2006) or in section 2(1) of the International Banking Order, 2000 (S 53/2000); and includes Islamic banking business as defined in section 2(1) of the Islamic Banking Order, 2008 (S 96/2008);

The following entities are included in the definition of financial institutions and are reporting institutions for Suspicious Transaction Reports (STRs):

- Banks
- Islamic Trust funds
- Insurance Companies, adjusters, brokers.
- Finance companies
- Investment advisers
- Investment dealers
- Money Changers
- Remittance Companies

4. What are suspicious transactions?

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 are suspicious transactions. There is no threshold for reporting STRs.

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.

To enable easier identification of inconsistent activity or behavior, it is important to undertake the following actions:-

- Ensure customer profiles are updated;
- Obtain records containing basic identification information, employment, other source of funds, nature of business/ use of any particular account, etc.; and
- Conduct transaction monitoring via an appropriate system or manually depending on the volume of transactions conducted.

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.

In most cases, it may not be possible to identify the actual criminal activity that is occurring. However, to assist in detecting suspicious transaction, reporting institutions 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 **Annex 1**. It may sometimes require a combination of the indicators to occur for it to be suspicious.

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 after 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 financial sector which can be used to enhance assistance by FIU to law enforcement agencies and feedback to the financial institutions.

5. When to report suspicious transactions?

All STRs should be submitted to the FIU within 5 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.

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

a) *Initial detection or alert of unusual transaction*- this can be from the frontliners or during monitoring of accounts;

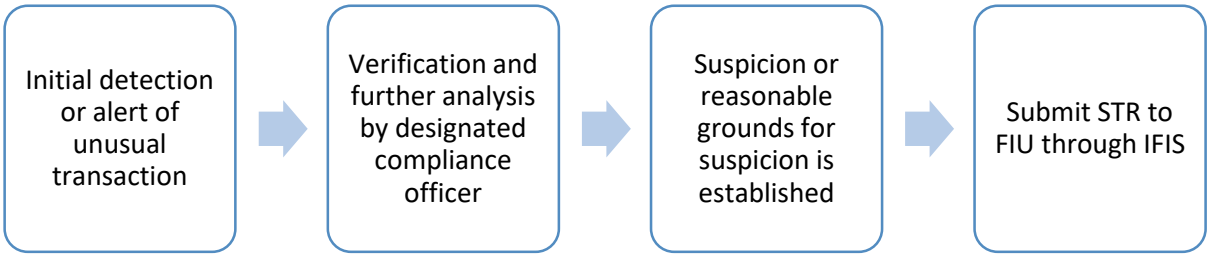
b) *Verification and further analysis by designated compliance officer* – this stage involves the financial institutions gathering and verifying information of the customer and transaction(s) to determine if the transaction is suspicious or if there is reasonable ground to suspect the transaction is linked to criminal proceeds or terrorism financing. Reporting institutions should demonstrate the time taken for this stage is effective and reasonable, and should not take more than **60 calendar days**. However, for transactions that are either cash intensive or involving overseas transfers or are suspected to be linked to high risk predicate offences[1], the time taken for this stage should not take more than **30 calendar days**;

c) *Suspicion or reasonable grounds for suspicion are established* – the moment compliance officer established suspicion or reasonable grounds to suspect the transaction is linked to criminal proceeds or terrorism financing. This may be the same time as the initial detection of the unusual transaction; and

[1] High risk predicate offences identified through the National Risk Assessment on Money Laundering and Terrorism Financing 2016 (NRA): Cheating, Criminal Breach of Trust, Corruption and Bribery, and Cigarette Smuggling.

d) *Submit STR to FIU through 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:



After an STR has been filed, reporting institutions 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.

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 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.

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

6. Failure to submit a suspicious transaction report

Failure to submit a report to the FIU is an offence and if found guilty is liable to a fine not exceeding $50,000, imprisonment for a term not exceeding 5 years or both.

7. Tipping Off

Confidentiality of STR information is crucial in protecting the interest and security of the financial institutions, the compliance officers, the FIU and the public. STR information contains private and sensitive financial information as well as unproven allegations of individuals and entities. Confidential breaches may undermine the suspicious transaction reporting system and any prevention of criminal activities that could have been resulted from the STR.

Tipping off is one of the several measures provided by CARO in protecting the confidentiality of STRs. Once an STR is submitted to the FIU, financial institutions or DNFBPs, including director, partner, officers, principal 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.

Financial institutions 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.

For financial institutions that are a branch or subsidiary with its 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.

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

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

Any person found disclosing information that a report has been made or an investigation is being or has been carried out to the customer or any other third party, is guilty of tipping off and is liable to a conviction to a fine not exceeding $500,000, imprisonment for a term of 5 years or both.

8. How to report STR?

STRs are to be submitted online through the Integrated Financial Intelligence System (IFIS) website (https://ifis.ambd.gov.bn) using one of the following methods:

i. **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.

ii. **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 reporting institutions.

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

9. What to include in an STR?

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.

The items below are the minimum technical requirements in submitting an STR:

a) Identification information such as:
   - For Individuals – Full name, IC no., etc
   - For corporations – Full name, date and place of incorporation and if possible, details of beneficial owners/directors and shareholders.

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

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

d) 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.

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

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

a) **Who** is involved: In addition to providing identification information in the appropriate fields in an STR report, 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.

b) **What** activity is occurring: In addition to any transaction input in the STR the narrative should point out what kind of transactional 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 (eg. If they were uncooperative), and actions by the teller, relationship manager or any officer that was involved over the course of establishing suspicion.

c) **When** is the activity 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.

d) **Where** is the activity occurring: There should be an indication of where the activity is occurring eg. At X district or X branch.

e) **How** is the activity 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) or other means (e.g. Over the phone)

f) **Why** the bank has considered the transaction or attempted transaction suspicious, including:

   a. Indication of serious offence, if apparent eg. 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.

It is important that financial institutions 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.

10. What happens after an STR is received by FIU?

STRs received from reporting entities are analysed to determine if activities conducted by the reported individuals involved are suspicious or is 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 our analysis process.

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.

11. Feedback

The FIU may provide the following feedback:

- **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 reporting institutions in reporting future suspicious activity and a better understanding of a good STR. Generally, the better quality of an STR, the better quality STR will assist in better understanding/faster analysis and action on the suspicious activity.

- **Trends and typologies**
  The FIU will provide feedback of common indicators or current trends and typologies observed from the different STRs received from different reporting entities. 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.

- **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.

12. Comments?

These guidance paper will be reviewed on a periodic basis. If you have any comments or suggestions to help improve this paper, please send your comments by email to fiu@ambd.gov.bn.

13. How to contact the FIU?

For further information on STR submission, please contact the FIU at:

Financial Intelligence Unit
Autoriti Monetari Brunei Darussalam
Level 7, Ministry of Finance Building
Commonwealth Drive
Bandar Seri Begawan BB 3910
Brunei Darussalam
Tel: +673 2382614

14. Revision History

Version	Date	Remarks
1.0	16 March 2017	New document
1.1	21 November 2019	Amendments made: 1. Section 5 – Time taken for verification and further analysis by designated compliance officer leading up to the submission of STR. 2. Section 7 – Sharing of private or sensitive information by a financial institution in Brunei Darussalam that is a branch or subsidiary of a foreign company with its compliance function located overseas.

Annex 1

LIST OF RED FLAG INDICATORS

* this list is not inclusive and may be updated at any time

GENERAL

1) Customer admission of criminal activity
2) Adverse reports – international
3) Adverse reports on commercial databases
4) Adverse reports on local press
5) Appear on OFAC or other list
6) No economic justification
7) Physical cash presented in unusual condition
8) Purchase of real estate without seeing the property
9) Early surrender of insurance
10) Use of gatekeepers
11) Use of Hawala or alternate money remittance
12) Use of new payment technologies / methods
13) Use of nominees and trusts
14) Use of offshore financial services
15) Use of personal account instead of business
16) Use of shell companies
17) Use of virtual currency or cryptocurrency
18) Use of casinos and gaming activities
19) Suspect has a criminal record
20) Suspect is a foreigner or non-resident
21) Customer is a public servant
22) Customer is unemployed, a housewife, student, retiree or pensioner
23) Use of charity (Non-Profit Organisations)

DOCUMENTATION

24) Discrepancies in supporting documents
25) Use of falsified documents
26) Suspect uses different names on sales agreement and payment
27) Use of family members and third parties
28) Source of funds is from another bank

CUSTOMER BEHAVIOUR

29) Suspect is reluctant to explain their transactions
30) Suspect refuses to provide further information
31) Suspect does not know how much money is being exchanged
32) Suspect does not know details of transaction (e.g beneficiary and source of fund)

33) Suspect gives conflicting explanations of transaction(s)
34) Suspect is an Insider no longer affiliated with your institution
35) Suspect is an Insider still affiliated with your institution
36) Suspect seems to act on behalf of third party
37) Participation in organised criminal group / racketeering
38) Customer initiated the closing of account(s)

TRANSACTION

39) Activity does not match client profile
40) Currency exchange is done for a third party
41) Dormant account suddenly active
42) Early settlement of term loan/ financing
43) Exchange of low denomination notes to high denomination notes ('refining')
44) Explosive growth in company account over short period of time
45) High frequency of cash deposits
46) Income is disproportionate to business activity
47) Insurance premiums are paid by companies abroad
48) Large purchase(s) made with cash
49) Money transfer is done for a third party
50) Multiple just-below threshold transactions
51) Multiple transactions in round denominations
52) Multiple transfers to the same beneficiary
53) Receiving money transfers from high risk countries
54) Dealings with a Shell Bank
55) Smurfing – multiple financial transactions conducted by different individuals or entities what would otherwise be a large transaction that can be conducted by one person.
56) Structuring- to break large financial transaction into a series of smaller transactions to avoid reporting requirement
57) Sudden increase in activities
58) Transaction amount is disproportionate to income
59) Transaction conducted by 3rd party that have no apparent connection
60) Transactions involve jurisdictions with poor AML/CFT regime
61) Transfer of funds between company accounts (SDN BHD to non-SDN BHD)
62) Transfer of funds between a company to a personal account
63) Use of business account instead of personal
64) Use of minor accounts
65) Over Credit Limit Threshold in Credit Cards
66) Cash deposits with no rationale
67) Cash withdrawal immediately following a large inward transfer
68) Multiple transfers to a beneficiary from various persons

69) PEP's account sees purchases beyond salary deposits
70) Purchase of bulk goods from a personal account
71) Transfer of funds have no clear economic purpose
72) Transfer of funds overseas immediately following a large inward fund transfer
73) Transfer of funds overseas to a high-risk jurisdiction or sanctioned country
74) Transfer of funds overseas to a high-risk corporate vehicle (trust company)
75) Money mule (i.e. the account owner)
76) Proliferation financing
77) Involves international PEPs
78) Involves local PEPs
79) Purchase of securities or high value goods
80) Denomination conversion
81) Use of personal account instead of business
82) Cash settlement of term loan/financing
83) Cash settlement of credit card debt

Date: 21 November 2019