Financial Intelligence Agency
BERMUDA

GUIDANCE NOTES

DIGITAL ASSET BUSINESSES

VERSION 2.0

PUBLISHED – MARCH 2026

FINANCIAL INTELLIGENCE AGENCY BERMUDA

SECTOR SPECIFIC GUIDANCE NOTES FOR DIGITAL ASSET BUSINESS FOR FILING A GOOD QUALITY SUSPICIOUS ACTIVITY REPORT (SAR) AND SUSPICIOUS TRANSACTIONS REPORT (STR)

The Financial Intelligence Agency (FIA) was established by the Financial Intelligence Agency Act 2007 to act as an independent agency authorized to receive, gather, store, analyse and disseminate information relating to suspected proceeds of crime and potential financing of terrorism received in the form of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs). The FIA only accepts SARs and STRs that have been submitted electronically via the FIA's designated platform (currently goAML) using the online submission form or XML transmission. In exceptional circumstances, an alternative method can be provided.

This document contains information that will assist persons with their reporting obligations pursuant to the Proceeds of Crime Act 1997 (POCA) Sections 46 and 47, and Anti-Terrorism (Financial and Other Measures) Act 2004 Sections 9,10 and 10A. This guidance does not represent legal advice. If you are unsure about your obligations in a specific case, please seek independent legal advice.

Bermuda Personal Information Protection Act (PIPA) and SAR/STR Reporting

The Bermuda Personal Information Protection Act 2016 (PIPA) establishes a framework governing the collection, use, and disclosure of personal information by organisations operating in Bermuda. PIPA requires that personal data be handled in accordance with established privacy principles, including obtaining consent and limiting disclosure to purposes for which the information was originally collected. Financial institutions and other reporting entities must be mindful of their obligations under PIPA when handling client data in the ordinary course of business.

However, obligations arising under Bermuda's anti-money laundering and anti-terrorist financing regime — including the duty to file SARs and STRs pursuant to the Proceeds of Crime Act 1997 and the Anti-Terrorism (Financial and Other Measures) Act 2004 — take precedence over the privacy protections afforded by PIPA. Section 55 of PIPA expressly provides for exemptions where disclosure is required or authorised by law, which encompasses the statutory obligation to report suspicious transactions to the Financial Intelligence Agency (FIA). Accordingly, reporting entities must not allow PIPA considerations to impede or delay the filing of a SAR/STR, and no client consent is required — nor should it be sought — when making such a report. The tipping-off provisions further underscore this point: notifying a client that a SAR/STR has been filed is itself a criminal offence, reinforcing that the duty to report operates independently of, and overrides, any data privacy obligations under PIPA.

Published – March 2026

TABLE OF CONTENTS

1. PURPOSE OF A SAR AND STR REPORT

The purpose of the Suspicious Activity Report (SAR) and Suspicious Transaction Report (STR) is to alert the FIA that certain client/customer or related business activity is in some way suspicious and might indicate money laundering or financing of terrorism. The information provided in these reports play a vital role in aiding law enforcement in money laundering (ML), terrorist financing (TF) or proliferation financing (PF) investigations and assisting with identifying emerging trends and patterns connected to financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to stakeholders. Reporters are required to submit reports that are complete, accurate, and filed promptly. Therefore, it is crucial that Money Laundering Reporting Officers (MLROs) and/or Nominated Officers (filers) provide narratives that are clear and comprehensive. The failure to adequately describe the indicators making the transaction or activity suspicious, delayed reporting and absence of supporting documentation undermines the purpose of the SAR/STR and minimizes its usefulness to law enforcement. Reports are reviewed and analysed by the FIA Analysts, who then disseminate the relevant intelligence/information, if warranted to the relevant law enforcement agencies, whether domestic or foreign to initiate potential investigations.

Reports filed with incomplete data will be rejected.

Individuals filing or reporting SAR/STRs to the FIA are guided to PRINT or SAVE a copy of their SAR/STR prior to final submission if desired. Once the SAR/STR has been approved, it will no longer be visible.

2. DEFINING SAR AND STR

A **SAR** details suspicious activity that does not currently contain any financial transactions. For example, declined business, dubious emails and requests, strange phone calls and the suspect comportment or associations of a subject or entity can be detailed in a SAR.

A **STR** details suspicious activity that involves a financial transaction. For example, unusual transactions that deviate from known client activity, unexplained large cash deposits, transactions which have no apparent lawful purpose and transactions to high-risk jurisdictions. Financial transactions are to be input into goAML to support the STR narrative along with the relevant supporting documentation.

3. QUALITY OF SARs/STRs

The FIA may reject the filing of a poor-quality or incorrectly filed report and advise the reporter to resubmit the report within five calendar days. The rejected report can be found in the draft section of the goAML platform. If a resubmission is not received before the end of five calendar days, the report will be archived, and a new SAR/STR will need to be submitted to the FIA. The FIA cannot interpret, assume, or infer what suspected money laundering, terrorist financing, and/or predicate offence the reporter believes may have been committed. The FIA may also refer the consistent reporting of poor-quality SARs/STRs to the relevant supervisory body for its attention and appropriate action.

4. TIPPING OFF

Bermuda legislation requires that a financial institution, its directors, officers, employees, and agents who, voluntarily or by means of a suspicious activity report/suspicious transaction report, report suspected, or known criminal violations or suspicious activity **may not** notify any person involved that the transaction has been reported.

5. DEVELOPING THE SAR/STR NARRATIVE

The SAR/STR report narrative should be provided in the 'REASON FOR SUSPICION' section of the submitted SAR/STR forms within the goAML platform. This narrative/ reason acts as a summary of the suspicious activity or transaction being reported. It should contain enough information for the FIA to analyse alongside the supporting documentation. It is vital for the reporting party to bear in mind that the Analyst handling the disclosure may nit be familiar with the specifics of your business or have in-depth understanding of your client. Therefore, it is essential to clearly detail the relationship between your business and the named subjects within the report, and to include information on any services provided to these subjects. Without this information, it can be challenging for the Analyst to fully comprehend the reported matter.

If the reporting entity has engaged with law enforcement prior to submitting a SAR/STR, this should be noted in the narrative, along with relevant contact details. The report should also include contact information for the primary and secondary contacts of the reporting party, specifying which individual is responsible for each report. Please attach a copy of the internal SAR but ensure that your narrative is clearly stated in the "reasons for suspicion" section

Avoid acronyms and jargon – they may not be understood by the recipient and are open to misinterpretation. If describing a service provided or a technical aspect of your work, please provide a brief synopsis in your SAR/STR to aid the reader.

Previous SAR/STR reference if the subject has been the subject of a SAR/STR.
As a basic guide, wherever you can, try to answer the following six questions to make the report as useful as possible:

5.1. WHO is involved?

Include the full legal name and address of the client, and length of the business relationship. For corporate clients, include both their registered office address and address of operation if different.

The following should be included when identifying involved parties:

- Include the full legal name, known aliases,
- Date of birth of all individuals involved in the suspicious activity or transaction,
- Their employer and occupation, title held,
- Business and residential address(es)
- Indicate domestic or foreign Politically Exposed Persons are involved,
- Outline the relationship between involved persons (i.e. business associates, colleagues, familial relationship).

If the reported subject (e.g. client/customer) has been the subject of a previous SAR/STR submitted by your organisation, please include previous FIA references numbers.

5.2. WHAT is the activity or transaction?

Describe the suspicious activity or transaction, the criminal property involved, its monetary value and source and ultimate use of funds. it is also important to note WHAT instruments or mechanisms were used to conduct / facilitate the suspicious activity e.g., bank account, wire transfers, companies, insurance policies, debit or credit cards, digital wallets and other assets businesses services etc.

5.3. WHERE did the activity or transaction take place and where are funds involved held?

Provide the location of the activity or transaction. Indicate all local and international financial institutions involved, type of account (personal or corporate), and corresponding account numbers.

5.4. WHEN did the activity or transaction take place?

Indicate the date of the activity and duration. If the activity takes place over of period, clearly identify the date the suspicious activity was detected. If there are multiple transactions to report, please enter each in a chronological order with individual dates and amounts under the transactions section.

5.5. WHY are you suspicious?

Clearly identify WHY the activity is considered suspicious, and what are the reasons for reporting. Provide a brief description of the nature and purpose of the client account to which to the suspicious activity or transaction relates. Include reasons and indicators for suspicion outlining the inconsistency with the client's profile, normal behaviour, and business activity. Follow up actions such as intent to terminate business relationship and close client accounts should also be included.

5.6. HOW was the activity or transaction executed?

Provide details on how the activity or transaction occurred.

6. EXAMPLES OF COMPLETE AND INCOMPLETE REPORTS

6.1. EXAMPLES-DIGITAL ASSET BUSINESSES

Incomplete DAB SAR/STR

INCOMPLETE DIGITAL ASSET BUSINESS SAR /STR

Narrative

This SAR is being filed for suspicion concerning the source of funds in Balan SIRBU'S account. SIRBU's account was created on 08/24/2015 using email address Sirbu2605@gmail.com. SIRBU was identified to be a true match to an individual who was arrested in Nanded, India in April 2017 for proliferating child pornography.

Complete DAB SAR/STR

COMPLETE DIGITAL ASSET BUSINESS SAR /STR

Narrative

Due to the inherent nature of cryptocurrencies, most transactions executed on the blockchain are public and can therefore be investigated using blockchain analytics tools such as our in-house tracking tool. As a result, transactions can be frequently linked to other cryptocurrency exchanges, markets (including darknet markets), or specific individual actors.

INCOMPLETE DIGITAL ASSET BUSINESS SAR /STR (Cont'd)

He allegedly operated a subscription-based website providing services in uploading and downloading audio and video files of child pornographic materials to customers.

While SIRBU's pattern of activity does not itself raise flags, suspicion concerning the source of funds was raised following open-source intelligence results indicating his arrest and that his website and its hosting provider, BITBOT, accept cryptocurrency as payment.

These findings increase the likelihood that the cryptocurrency deposited to the account are proceeds from the operation of the child pornography site, especially given that all activity occurred between 13-Sep-2016 and 03-Mar-2017 prior to SIRBU's arrest in April 2017. The total value of SIRBU's deposits amounts to **USD187,046.22**. Sirbu's account is disabled with no balance.

Action
Account has been terminated

goAML Indicators selected
Adverse Media
No Source of Funds

Supporting Documents provided
- Internal SAR
- Account activity screenshot

Missing Information
- Subject identification
- Name of website
- Date of detection of the suspect activity was not mentioned in the SAR narrative
- No Report Indicators were selected

COMPLETE DIGITAL ASSET BUSINESS SAR /STR (Cont'd)

The subject, Ms. Teresa Renalda CORREIA created a cryptocurrency account on 08-Oct-2021 and is suspected of using her account to potentially launder funds.

Our transaction monitoring system triggered as Ms. Teresa Renalda CORREIA's transactional activity showed the following:
- Crypto In Crypto Out- customers receive crypto and sends crypto of comparable value off platform within a short period and multiple number of times.
- High Risk Heavy Hitters-customers in High-Risk Assets and High-Risk Country Transactions based on the jurisdiction and domicile of the user which is Colombia.

A full review of the account identified the following suspicious activity:
- On 08/10/2021 Ms. Teresa Renalda CORREIA had received 5 amounts of Tether (USDT) totalling **USD239,658.48**.
- On 08/10/2021 Ms. Teresa Renalda CORREIA has sent **USD208,913.74** worth of USDT, via 3 separate transactions.

The currency was sent to and received from unlabelled wallets. It appears that these are unlabelled wallets which had interacted with known exchanges such as Binance and Gemini. Given the pattern observed on the account these unlabelled wallets are suspected to be owned by Ms. Teresa Renalda Correia. An Enhanced Due Diligence request to the determine the user's Source of Funds was attempted twice on 22-Jan-2022 and 29-Jan-2022, however no response was provided to date.

An open-source intelligence search did not reveal further information about Ms. Teresa Renalda CORREIA at this time.

Based on the narrative and the analysis set out, our internal review has identified suspicious activity on this account. The user did not respond to two attempts of Enhanced Due Diligence to determine their source of funds and wealth. Ms. Teresa Renalda CORREIA's account activity is deemed suspicious, as there is a consistent pattern of flow through Crypto In Crypto Out, this activity happened in one single day, 17/11/2023 which happens to be the same day the user's account was created and no other transactions have been seen on the account since then. The user did not respond to two attempts of Enhanced Due Diligence (EDD) to determine their source of funds and wealth. These activities raise money laundering concerns with Ms. Teresa Renalda CORREIA's account.

7. SUPPORTING DOCUMENTS

All documents referenced in the submission, and which were crucial in forming your suspicion and creating the filing should be attached to the original submission. The following key documents should also be considered when submitting a SAR/STR to determine if they provide confirmation or clarification of the report and would reduce the need for the FIA to make formal requests minimizing the time to complete the analysis. The FIA understands documentation may be limited depending on the relationship with the subject(s) being reported.

COMPLETE DIGITAL ASSET BUSINESS SAR /STR (Cont'd)

Action
Account was terminated on February 15, 2022

goAML Indicators selected
- Cryptocurrency/Bitcoin
- Inconsistent Account Activity
- Morality Related
- No Source of Wealth
- No Source of Funds
- Refusal to comply with KYC requirements

Supporting documents provided
- Account activity
- Teresa Renalda CORREIA's identification

7.1. Natural Persons

- **MANDATORY -** Certified passport or other government issued identification for all citizenships held
- **MANDATORY -** Certified proof of residential address
- Declaration of source of wealth/funds where available
- Account initiation forms, once available stating purpose of account (s) and source of funds.

7.2. Trusts and Foundations

- Certified extract of original Deed of Settlement detailing Settlor, Beneficiaries, Protector/Enforcer
- Supplemental Deeds showing any changes to the original Deed of Settlement
- **MANDATORY -** Certified Due Diligence (Government issued identification showing full name; proof of residential address) for all named persons in items 1 & 2
- Most recent financials (list of all assets held)
- Source of wealth/funds
- **MANDATORY -** Evidentiary correspondence that contains supporting details, suspicious requests, incriminating statements
- Internal SAR

7.3. Corporate Entities

Where the subject may be a retail entity, please provide the equivalent documentation.
- Certificate of Incorporation
- Directors & Officers Register
- Share Register

- **MANDATORY -** Confirmation of registered address, principal business address and mailing address (if different from the registered address)
- **MANDATORY -** Certified due diligence (Government issued identification showing full name; proof of residential address) for all named persons in items 2 & 3. For item 3, where interest held is 10% or more.
- Ownership structure chart
- Most recent financials (list of all assets held)
- Source of wealth/funds
- **MANDATORY -** Evidentiary correspondence that contains supporting details, suspicious requests, incriminating statements
- Internal SAR

7.4. Non-Profit Organizations

- Register of Directors or Trustees
- **MANDATORY -** Certified due diligence (Government issued identification showing full name; proof of residential address) for all named persons in item 1.
- Most recent financials (list of all assets held)
- Source of wealth/funds
- **MANDATORY -** Evidentiary correspondence that contains supporting details, suspicious requests, incriminating statements
- Internal SAR

8. RETENTION PERIOD

Financial institutions shall retain the following for five years from the date of the filing:

- A copy of all filed SARs/STRs
- The original or business record of any supporting documentation
- All supporting documentation for the benefit and/or use of the FIA and any other appropriate local law enforcement agency or regulatory authorities.

9. SEEKING CONSENT TO CONDUCT A TRANSACTION

For detailed guidance on seeking Consent, please refer to our standalone Consent Guidance document which is available on the FIA's website at https://www.fia.bm/consent-regime/.

10. RED FLAG INDICATORS

The following list is not exhaustive and may be updated as emerging money-laundering and financing of terrorism trends and patterns evolve. The existence of an indicator may not alone imply suspicion but combined with other indicators may suggest a suspicious transaction.

10.1. Red Flag Indicators for Digital Asset Business

1. Client provides false or misleading information
2. Unusual or suspect source of funds or refusal to provide source of funds information
3. Client is unwilling, unable or uncontactable to provide information for CDD purposes
4. Complex or layered ownership structure for no apparent economic or business purpose
5. Client linked to adverse media relating to a suspect activity or law enforcement investigation
6. Client resides in or the transaction involves a jurisdiction known to have inadequate anti-money laundering and counter financing of terrorism framework or a jurisdiction in which the FATF has called for countermeasures or enhanced client due diligence measures
7. Conducting a large initial deposit to establish a new relationship with a DAB and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most digital assets have a transactional limit for deposits, laundering in substantial amounts could also be done through over-the-counter trading.
8. Conducting digital asset to fiat exchange at a potential loss (e.g. when the value of digital asset is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).
9. Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use digital assets instead of fiat currency
10. Structuring digital asset transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions
11. Abnormal levels of low-value or high-value transactions into the same account in short succession particularly from unrelated wallets or where there is no activity for an extended period afterwards
12. Transferring digital assets immediately to multiple digital asset service providers, including those registered or operated in other countries where there is no relation to the customer's country of residence or business or where there is inadequate anti-money laundering and counter financing of terrorism framework
13. Transactions involve multiple digital assets, or multiple accounts, without a logical business explanation
14. Digital assets moved from a public, transparent blockchain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin
15. Digital assets traded to or from wallets that indicate the use of mixing or tumbling services or peer-to-peer platforms

16. Customers that operate as an unlicensed digital asset service provider on peer-to-peer exchange website
17. Abnormal transaction activity of digital assets from peer-to-peer platform associated wallets with no logical business explanation
18. Use of cross-chain swaps within VASPs (e.g. receiving Ethereum-based tokens but withdrawing Tron-based ones)
19. Transactions involving more than one type of digital assets particularly those that provide higher anonymity, such as anonymity enhanced cryptocurrency or privacy coins and despite additional transaction fees
20. Customer funds originate from, or are sent to, an exchange that is not registered in the country where either the customer or exchange is located
21. Receiving or sending digital assets to or from darknet marketplaces or using virtual assets whose design is inadequately documented and possibly linked to fraudulent activities such as Ponzi schemes and ransomware.
22. A large number of seemingly unrelated digital asset wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other
23. Using digital asset ATMs/kiosks despite the higher transaction fees and including those commonly used by mules or scam victims or ATMs/kiosks in high-risk locations where increased criminal activities occur. Note: a single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors)
24. Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious or transactions to open an account frequently within the same digital asset from the same IP address
25. Merchants or corporate users' internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration
26. Customer is significantly older than the average age of platform users or who appears unfamiliar with digital asset technology opens an account and engages in large numbers of transactions, suggesting their potential role as a digital asset money mule or a victim of elder financial exploitation

For a more extensive list of red flags ML/TF indicators categorised, consult the FIA's Indicators list document located on its website HERE.

11. REPORTING RESPONSIBILITIES

It is the responsibility of all Bermuda-supervised reporting entities to ensure that a Reporting Officer (Money Laundering Reporting Officer (MLRO)) is appointed or designated and is adequately trained, in accordance with section 17(1) and (3) of the Proceeds of Crime Act 1997.

The MLRO must be registered with, and have access to, the Financial Intelligence Agency of Bermuda's designated reporting platform in order to submit Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) where the reporting officer knows, suspects, or has reasonable grounds to suspect that a person or entity is engaged in money laundering or terrorist financing.

It is strongly recommended that reporting entities establish internal policies and procedures to ensure that:

1. A Reporting Officer (MLRO or other designated reporting person) is appointed at all times.
2. An Alternate Reporting Officer is registered and authorised to submit reports in the absence of the Reporting Officer.
3. The Reporting Officer and/or Alternate Reporting Officer are adequately trained to use the FIA's reporting system, submit SARs/STRs, and receive and respond to additional requests from the FIA, including requests made pursuant to section 16 notices;
4. A group notification email address is maintained to ensure that the compliance department, or other designated personnel, receive all confirmations of receipt and follow-up communications issued by the FIA.
5. In the event of the departure, resignation, or termination of the MLRO or Alternate MLRO, the reporting entity must immediately appoint a suitably trained replacement and ensure continuity of reporting obligations through the FIA's designated reporting platform.

12. goAML SUPPORT CONTACT DETAILS

For assistance registering on goAML platform or with submitting SARs and STRs, the FIA can be contacted as follows:

Tel: 441-292-3422 ext. 8005 (Option 3)
Email: goaml_support@fia.bm

-END-