GUIDANCE NOTES

HIGH VALUE GOODS DEALERS

VERSION 2.0

PUBLISHED – MARCH 2026

FINANCIAL INTELLIGENCE AGENCY BERMUDA

SECTOR SPECIFIC GUIDANCE NOTES FOR HIGH VALUE GOODS DEALERS 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, terrorist financing, fraud, and other financial crimes. 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, concise, 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 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. Once the SAR/STR has been approved, it will no longer be visible to the filer.

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 must be entered 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 not be familiar with the specifics of your business or have an 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 party 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?

Identify the client to which the suspicious activity relates, including the full legal name, address, and length of the business relationship. For corporate clients, include both their registered office address and address(es) 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, occupation, and title held
- Business and residential address (es),
- Indicate whether domestic or foreign Politically Exposed Persons (PEPs) 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. Clearly outline what instruments or mechanisms (including structures, administrative services, or service delivery channels) were used to conduct or facilitate the suspicious activity e.g. bank account, wire transfer, companies, debit or credit cards, digital 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 its duration. If the activity takes place over a period of time. If there are multiple transactions to report, please do so in chronological order with individual dates and amounts.

5.5. WHY are you suspicious?

Clearly identify WHY is the activity considered suspicious, and what are the reasons for reporting. Provide a brief description of the nature and purpose of the client business relationship 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-High Value Goods Dealers

Incomplete HVGD SAR/STR

INCOMPLETE HVGD SAR /STR

Narrative

We received a request from Jeff HOLMAN, a British citizen, to aid in the sale of five paintings worth $718,000.00. HOLMAN had been in contact with two potential buyers and asked for the sale of the proceeds to be sent to an account in Geneva, Switzerland. The private individual who wished to buy three paintings was to remit funds from a corporate account in Panama with the paintings sent to the Thames Freeport in London, England. We are reporting this as we believe there could be an attempt to avoid import and other taxes as well as potential money laundering.

Complete HVGD SAR/STR

COMPLETE HVGD SAR/STR

Narrative

On July 31, 2023, a customer visited our store to inquire about a special-order custom gold and diamond men's necklace and pendant. He was advised that the items would take 4-6 weeks from design to creation, and to begin the process he must complete our special-order form and pay a 30% deposit. The form was initially completed with the alias "Hawk"; we asked for his legal name to be noted on the form, at which point he noted his name was Dean WILLIAMS. Mr. WILLIAMS was advised that the custom items would cost $11,000.00 He paid the deposit of $3,300 in cash. Our sales lady informed Mr. WILLIAMS that the

***INCOMPLETE* HVGD SAR /STR (cont'd)**

goAML Indicators selected
- Tax Evasion
- Money Laundering

Supporting documents provided
None.

Missing Information
- Narrative Detail –
  - Outline of actions or behaviours that caused suspicion
  - Indication on status of the sale – complete, declined, in progress
  - Dates of the communication
  - Details of the potential buyers
- Internal SAR

***COMPLETE* HVGD SAR/STR (cont'd)**

Narrative (cont'd)

balance of funds would be due upon collection of the items, and he could choose to pay by card or online transfer.

On September 5, we called to confirm the order was ready for collection. When Mr. WILLIAMS attended the store, he had the balance of the payment $7,700.00 in cash. The sales lady noted that the cash was a little worse for wear and inquired where the cash came from. Mr. WILLIAMS responded that he owned his own landscaping company, presented a business card in the name of ECO LANDSCAPING SERVICES BDA, and stated that most of his residential clients pay him in cash, and he had been saving up for a while. The sales lady then advised that it was store policy not to accept cash payments more than $5,000.00 and inquired if he had a debit or credit card he would like to use. Mr. WILLIAMS became very irritable stating that he would be willing to pay an additional $500.00 if the cash payment could be accepted and further suggested we could then record it as two smaller payments so it would adhere to the store policy. Mr. WILLIAMS was told that would be inappropriate, was again asked about using a bank card, and was provided with the store's bank transfer details. The sales lady informed the store manager about both interactions with Mr. WILLLIAMS.

On September 8, the balance owing was received from a bank account in the name of Shalita T.J. FRANCIS, who is unknown to us. Mr. WILLIAMS visited our store to collect the necklace on September 9 at which time he was asked by our part time salesperson to provide identification in order to collect. Mr. WILLIAMS was initially hesitant to provide an ID and stated he had just been in the store the day a few days before so we should know him. The salesperson responded that she was unfamiliar with the transaction and needed to make sure she was giving the expensive item to the correct person. Mr. WILLIAMS provided his driver's licence and left the store after receiving the necklace and pendant.

Action
The store manager advised his team to make a copy of Mr. Williams' identification when he returned to collect as his behaviour raised suspicions that he could be involved in money-laundering.

goAML Indicators selected
- Suspect Comportment
- Cash Purchase
- Money Laundering
- Cash Deposit - unable to identify third party.

Supporting documents provided

Special Order form
Deposit receipt
Screenshot of incoming funds
Copy of landscaping business card
Copy of driver's licence-Terrence Dean Williams
Internal SAR including photo of necklace

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.

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

7.2. Trusts and Foundations

- Certified extract of original Deed of Settlement detailing Trustee, Settlor, Beneficiaries, Protector/Enforcer or Foundation Constitution
- 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.

10. RED FLAG INDICATORS

The following lists are 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 High Value Goods Dealers

1. Large cash transactions or use of large denomination bank notes
2. Unusual or suspect source of funds or refusal to provide source of funds information
3. Transaction is beyond the legitimate means of the client based on known income
4. Willingness to pay higher cost to expedite transactions without a plausible explanation or to conceal beneficial owner identity
5. Client is suspected to be conducting transactions on behalf of a third party without identity disclosure
6. Client provides false or misleading information
7. Frequency of transactions exceeds normal levels for transaction type

8. Transactions suspected to be in violation of another country's foreign exchange laws and regulations
9. Under- or over-valued transactions
10. Request for "off the record" transaction
11. Request to refund overpayment to a third party
12. Excessive inquiries about refund policies and subsequent request for large refund
13. Transaction involves unusual or complex payment arrangements for no apparent economic or business purpose
14. Client is unusually persistent in requesting to purchase goods from a specific staff member at a specific location when the same item is readily available at a branch closer to where they live.
15. Client is unwilling, unable, or uncontactable to provide information for CDD purposes
16. Politically Exposed Persons particularly where status is undisclosed or denied
17. Client linked to adverse media relating to a suspect activity or law enforcement investigation
18. 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

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-