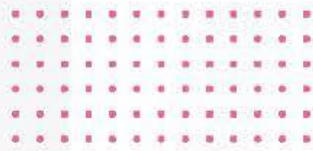




GUIDANCE NOTES

INSURANCE SECTOR



VERSION 2.0

PUBLISHED – MARCH 2026



FINANCIAL INTELLIGENCE AGENCY BERMUDA

SECTOR SPECIFIC GUIDANCE NOTES FOR LONG-TERM INSURERS, INSURANCE MANAGERS AND BROKERS 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 5
- 2. DEFINING SAR AND STR..... 5
- 3. QUALITY OF SARs/STRs 5
- 4. TIPPING OFF..... 6
- 5. DEVELOPING THE SAR/STR NARRATIVE..... 6
 - 5.1 WHO is involved?..... 6
 - 5.2 WHAT is the activity or transaction? 7
 - 5.3 WHERE did the activity or transaction take place and where are funds involved held? 7
 - 5.4 WHEN did the activity or transaction take place? 7
 - 5.5 WHY are you suspicious?..... 7
 - 5.6 HOW was the activity or transaction executed?..... 7
- 6. EXAMPLES OF COMPLETE AND INCOMPLETE REPORTS..... 7
 - 6.1 Examples- Insurance Managers..... 7
 - Incomplete Insurance Managers SAR/STR 7
 - Complete Insurance Managers SAR/STR 7
 - 6.2 Examples- Insurance Brokers 9
 - Incomplete Brokers SAR/STR 9
 - Complete Brokers SAR/STR 9
 - 6.3 Examples- Long-Term Insurers (LTIs) 10
 - Incomplete LTI SAR/STR 10
 - Complete LTI SAR/STR..... 10
- 7. 7 SUPPORTING DOCUMENTS..... 12
 - 7.1 Natural Persons..... 12
 - 7.2 Trusts and Foundations..... 12
 - 7.3 Corporate Entities..... 12
 - 7.4 Non-Profit Organizations..... 13
- 8. RETENTION PERIOD..... 13
- 9. SEEKING CONSENT TO CONDUCT A TRANSACTION 13
- 10. RED FLAG INDICATORS 13
 - 10.1 Red Flag Indicators for Insurance Managers, Brokers, and Long-Term Insurers 13
- 11. REPORTING RESPONSIBILITIES 15

12. goAML SUPPORT CONTACT DETAILS15

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 plays a vital role in aiding law enforcement in combating 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 minimises 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?

Include the full legal name and address of the Subject or client being reported, and length of the business relationship (including date of initiation 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:

- 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 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, insurance policies, 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 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- Insurance Managers

Incomplete Insurance Managers SAR/STR

Complete Insurance Managers SAR/STR

INCOMPLETE INSURANCE MANAGERS SAR /STR**Narrative**

We are writing to alert you to fraudulent cyber activity that has cost this firm \$4.23 million. This incident occurred in the context of an insured market loss warranty deal in October 2020 with our broker KEYON RE, and MINSHULL INDEMNITY, a property/casualty firm. KEYON RE'S principal, Keyon FELIX, resides in Florida. Our premium payment of \$4,230,000, intended for MINSHULL INDEMNITY, was diverted as a result of false bank account details KEYON RE provided to us, apparently because of a breach in KEYON RE's IT system. The hackers were able to exploit their unauthorized access to identify a legitimate deal in the works between this firm, KEYON RE and MINSHULL INDEMNITY.

Hackers impersonated MINSHULL INDEMNITY by using a fake domain to communicate the fraudulent account details to KEYON RE on September 30, 2020, at 12:16pm. In addition, the hackers apparently impersonated KEYON RE to pass on the account details to us on September 30, 2020 at 3:26 pm, and in purporting to confirm that on October 3, 2020 at 10:07am, that: "Yes I did a phone confirmation with them [MINSHULL INDEMNITY] on that, it is correct. They can proceed with the payment." We paid two wires in early October: one to KEYON RE for \$240,000.00; and another for \$4,230,000.00 to a bank account with Touchstone, a regional bank in Virginia.

On or about December 15, 2020, we learned that MINSHULL INDEMNITY, in conversations with KEYON RE at the end of November, discovered that the \$4,230,000.00 payment never arrived into MINSHULL INDEMNITY's account; but rather arrived into the account of a "TRIPPLE BENCH LLC" at Touchstone Bank in Virginia. Upon discovery, we commenced an internal investigation to look into the security of its systems and the payment of the wire in July. There is no indication of a breach of our systems or other suspicious activity within the system. We are, however, continuing to monitor systems for suspicious activity relating to KEYON RE, fake MINSHULL INDEMNITY accounts, and related suspicious activity.

Action

We commenced an internal investigation and continuing to monitor systems for suspicious activity.

goAML Indicators selected

- Scams – Identity Theft
- Scams – Investment related

Supporting Documents provided

None

Missing Information

- Email correspondence/ wire transfer details

COMPLETE INSURANCE MANAGERS SAR /STR**Narrative**

Our client, GIBBS RE requested a USD 482,973.00 wire payment to BARBARA PERRY & COMPANY ("BP&Co"), a US service provider to the client. The payment was executed according to instructions received, on 13 May 2024. On 30 May 2024, GIBBS RE notified us that the payment request was fraudulent.

An investigation was immediately launched into the payment and the circumstances surrounding it. This investigation included a review of the relevant emails and payment. As a result of its investigations, we understand that malicious actors compromised BP&CO's email systems.

We also understand that the email address from BP&CO purporting to provide payment details for the completion of the transfer was compromised and that the wire transfer details provided were fraudulent. It has also been confirmed that as of 3 June 2024, the full amount of the funds subject to the compromised transfer have been frozen by the recipient bank, BANK OF AMERICA whilst it conducts its own investigation into the fraudulent activity. We are currently collaborating with the client to assist with the recovery of these funds.

Action

An investigation is ongoing to gather all the facts and updates will be provided as required.

goAML Indicators selected

- Misrepresentation
- Scams - Business Email compromise (BEC)
- Electronic Transfers
- Fraud
- False Documents
- Use of Insurance Products

Supporting documents provided

- Internal SAR
- Wire transfer documents
- Fraudulent email request
- Correspondence with Bank of America

6.2 Examples- Insurance Brokers

Incomplete Brokers SAR/STR

INCOMPLETE INSURANCE BROKERS SAR /STR

Narrative

We, reinsurance broker CER Ltd registered in Bermuda, have received on August 20, 2023, from Simsek Insurance Company, an insurance company duly licensed under the laws of the sultanate of Oman, a request for broking the placement of a share of the reinsurance placement for a property insurance risk located in the sultanate of Oman.

The request which concerned the reinsurance of a share of that risk was sent to CER Ltd by Mr Yousef Mansour Kumar, reinsurance manager for Simsek Insurance Company.

During the exchanges with the above-mentioned person, and further to inquiries from our team regarding Simsek Insurance Company 's existing reinsurance panel for the already placed part of the proposed insurance policy, Mr Yousef Mansour Kumar unofficially disclosed through an instant messaging exchange with one of our employees that the company had independently secured other reinsurance support for various shares of the risk (copy of the placement table shared is attached) and needed our support for a remaining share.

The disclosure revealed that one of the shares Simsek Insurance Company had already placed or was planning to place representing 10% of the risk being covered seemed placed with or reserved for placement with Iran Insurance Company, an insurance company licensed under the laws of the Islamic Republic of Iran and owned by its government.

It was also worth noting that the involved insurer Simsek Insurance Company, a company listed under the Muscat Securities Market and regulated by the Omani regulator Capital Market Authority was onboarded by our company based among others on declarations alleging compliance with FATF policies, and their sharing of a "AML Procedural Manual" (copy attached).

While it is unclear whether this placement is final or a planned one, the sheer possibility of such a placement highlighted a dissonance with the declarations and policies shared by Simsek Insurance Company relative to compliance. Given the involvement of sanctioned entities as ultimate stakeholders, we hereby raise an SAR in view of the Money Laundering capability inherent to the arrangements referred above.

Complete Brokers SAR/STR

COMPLETE INSURANCE BROKERS SAR /STR

Narrative

An independent audit revealed discrepancies between new placement documentation and their corresponding payment records. A review of one randomly selected policy file showed that a brokerage client and policyholder, Jennifer COLT, paid \$5,311.00 on January 27, 2023, although the final executed policy documentation showed a premium of \$3,953.00, indicating a difference of \$1,358.00. Her client account did not show an overpayment as the \$1,358.00 had already been refunded to an overseas third-party account on April 5, 2023.

As this was an unusual occurrence, we contacted Jennifer COLT to verify the circumstances. The client insisted that they had not received a refund, confirmed their banking details and that their documentation showed a premium of \$5,311.00 was due. A further in-depth financial audit has revealed that Roger PILGRIM, one of our insurance brokers and Vanessa MITCHELL, a signing authority were engaged in dishonest conduct by overcharging clients for new placements. Roger PILGRIM requested the refunds which Vanessa MITCHELL then approved. To date, we have confirmed that they have diverted 48 client refunds to personal accounts totalling \$379,391.00.

As we are uncertain as to the full extent of the fraudulent claims, we are continuing an internal investigation.

Action

An internal investigation is ongoing to determine the full extent of the misconduct and updates will be provided as required. The Bermuda Police Service has also been advised. See attached correspondence for contact details of the officer overseeing the formal complaint.

goAML Indicators selected

- Misrepresentation
- Fraud
- False Documents
- Use of Insurance Products
- Theft

Supporting documents provided

- Extract of audit report
- Correspondence with Jennifer Colt
- Ledger of transactions involving Roger Pilgrim and Vanessa Mitchell
- Copy of premium payments
- Copy of refund transactions

INCOMPLETE INSURANCE BROKERS SAR /STR
(cont'd)

Note: at the time of this SAR, the property risk referenced “Sheikh Nasser Khawar Ahmed - Al Balushi Villa Phase (2) | MIC Ref. No. OFR-M-PAR-1328-09-05” has not been submitted to compliance screening yet.

Action
None

goAML Indicators selected
None

Supporting Documents provided

- Reinsurance placement table
- AML Procedural Manual

Missing Information

- goAML Indicators
- Correspondence with Yousef Mansour Kumar
- Onboarding documents of Simsek Insurance Company



6.3 Examples- Long-Term Insurers (LTIs)
Incomplete LTI SAR/STR

INCOMPLETE LTI SAR /STR

Narrative

Subject: Irshad Mohd Jilid Rahman
Date of Birth: January 20, 1989
Passport: Malaysia, #A59141215, Exp. March 24, 2028
Address: 8 Jalan Sungai Penchala, Desa Sri Har, Kuala Lumpur, Malaysia, 91630
Insurance Policy Number: 56211019
Policy Issue Date: June 23, 2015
Account Value: \$14,061,950.79
Death Benefit Amount: \$48M
Total Premiums Paid: \$11,211,975.00
Owner: CDS Group Holdings Ltd. Columbus Centre Road Town, Tortola, British Virgin Islands

Collateral Assignment: This policy is collaterally assigned to Hong Leong Bank Berhad (Singapore branch) and all funds will be paid to the owner’s (CDS Group Holdings Ltd.) account with Hong Leong Bank Berhad (Singapore Branch).

We received a request to surrender the above noted life insurance policy. The insured is the relative or close associate (RCA) of a PEP.

Complete LTI SAR/STR

COMPLETE LTI SAR /STR

Narrative

The Purpose of this STR is to provide information to the FIA regarding a Forced Full Surrender request for proceeds to be used to pay off the outstanding loans, imposed by the current Collateral Assignee bank, DBS Bank Ltd. for Life Policy 027112175 (Sun Global Legacy Plus III), valued at USD \$1,691,930 as of November 30, 2024. Surrender cash value USD \$1,562,110, funds pending consent process. Insured on policy is Ade K HIDAYAT (Subject 1) and Beneficiary Nurhayati W Hidayat (Subject 2).

A previous SAR was filed in July 2023 see attached below.

Since the previous filing additional details have been updated on Bridger Insight regarding August 2022 suspected embezzlement concerns. According to the report Nurhayati A HIDAYAT (Subject 2), was one of seven senior officials of PT PUTRI HADI NUR EFENDI (EFENDI LIFE) suspected in the alleged embezzlement case related to PT EFENDI LIFE. “All seven were suspected of violating a number of articles in Law Number 40/2014 concerning Insurance and Money

INCOMPLETE LTI SAR /STR (cont'd)

The PEP, Azfar Wahab Bala SARKAWI, is the insured's father-in-law, a former Minister, and a current Ambassador of Malaysia. While conducting due diligence in processing the surrender request, a Bridger watchlist scan re-confirmed the RCA match and did not note any negative news on the insured. However, an open-source search revealed a December 2023 article indicating that the Malaysian anti-corruption agency is preparing to charge the subject/insured with graft and criminal breach of trust (attached).

Action

Due to the timing of the surrender request and the pending criminal charges, we suspect that the Subject may have committed one or both of the following offences of the Proceeds of Crime Act: 43 (concealing or transferring proceeds of criminal conduct) and/or 45 (acquisition, possession or use of proceeds of criminal conduct).

goAML Indicators selected

- Adverse Media
- Corruption
- PEP Foreign

Supporting Documents provided

- Application for Life Insurance
- Irshad Rahman's photo identification
- Bridger scan

Missing Information

- Internal SAR
- Surrender Request
- Surrender docs
- Date of detection of the suspect activity was not mentioned in the SAR narrative

COMPLETE LTI SAR /STR (cont'd)

"Laundering Law of Criminal Code." The Financial Services Authority (OJK) has imposed sanctions on EFENDI LIFE for violating several rules. (See attached Bridger report for full details)

Action

An investigation is ongoing to gather all the facts and updates will be provided as required.

goAML Indicators selected

- Embezzlement

Supporting documents provided

- Previous SAR filing reference
- Email correspondence
- Client profile
- Bridger report
- 027112175 - Application
- 027112175 Broker Memo - Ade Hidayat
- 027112175 Source of Funds Initial Swift
- Ade Hidayat's Indonesia Passport
- 027112175 - Proof of Residential Address (PORA)
- Source of Wealth (SOW) - Ade Hidayat
- 027112175 - FINANCIALS
- 027112175 and 027102156 - Final SAR Report
- 027112175 - Global Investment Ltd - Self Certification
- 027112175 - Global Investment Ltd - Change form
- Interpol Red Notices

Additional supporting docs:

- 027112175 - Lifeware History
- 027112175 - Lifeware Overview
- 027102156 - Lifeware History
- 027102156 - Lifeware Overview
- 027102156 - Asep Enterprise Voi
- Dow Jones - Ade Hidayat
- Dow Jones - Nurhayati Hidayat
- TJE Corporate Directors PTE Ltd. Consent to act as Director
- Underwriting memo - Ade Hidayat
- WC Exact - Ade Hidayat
- 027112175 - Declaration of Corp. Partnership or Foundation

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 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
- 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 Insurance Managers, Brokers, and Long-Term Insurers

1. New or prospective client is known to you as having a questionable reputation or criminal background
2. Client shows uncommon curiosity about internal systems, controls, and policies
3. Client provides false or misleading information
4. Unusual or suspect source of funds or refusal to provide source of funds information
5. Client is unwilling, unable, or uncontactable to provide information for CDD purposes
6. Complex or layered ownership structure for no apparent economic or business purpose
7. Client linked to adverse media relating to a suspect activity or law enforcement investigation
8. Customer uses intermediaries which are not subject to adequate AML/CFT laws

9. 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
10. Customers that are legal entities whose structure makes it difficult to identify the ultimate beneficial owner or controlling interests. (Note: This can happen at inception or, subsequently, an individually owned insurance policy can be assigned to a legal entity. KYC/CDD processes should apply at both stages.)
11. Policy holder and/or the beneficiary of the contract are companies whose structure makes it difficult to identify the beneficial owner, e.g., multiple layers or because the entity's ownership structure crosses jurisdictions
12. Customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive
13. A customer relationship with the direct life insurer that does not appear to make economic sense, for example, the early redemption of a policy when the surrender value is less than the value of premiums paid
14. Transactions that are not commensurate with the customer's apparent financial means, for example, where customers without reasonable financial standing purchase large single premium policies for a large, assured sum
15. Large and regular premium payments that cannot be clearly identified as bona fide transactions, from countries or jurisdictions associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) other criminal conduct.
16. Source of premiums are from another country or jurisdiction with poor track record on CDD or record keeping requirements
17. Substantial increase in cash premium payments from foreign countries or jurisdictions by a customer without apparent cause, especially when such transactions are not consistent with the customer's transaction history
18. Request to refund overpayment to a third party
19. A history within an occupation with a higher risk for ML/TF due to local crime typologies, high access to cash-based businesses or international exposure
20. Gatekeepers such as accountants, lawyers, or other professionals holding accounts/policies/contracts at an insurer, acting on behalf of their customers, and where the insurer places unreasonable reliance on the gatekeeper
21. Payments are regularly received from third parties that are no apparent relationship with the policy holder
22. Policies managed by external asset managers who may not be adequately regulated and supervised
23. Customer (typically aged about 17-26) purchases a life policy with cash value and surrenders it within a short period, which could be an indication of terrorism financing
24. Agents who have consistently high activity levels of single premium business far in excess of any average company expectation
25. Policyholder may exercise cancellation rights or cooling off rights on life insurance products where the sum invested must be repaid (subject to any shortfall deduction where

applicable). This could offer a readily available route for laundering money, and insurers should therefore be alert to any abnormal exercise of cancellation or cooling off rights by any policyholder. If abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported through the usual channels

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-

