



---

**ANTI-MONEY LAUNDERING, COMBATting THE FINANCING OF  
TERRORISM AND THE PROLIFERATION OF WEAPONS OF MASS  
DESTRUCTION (AML/CFT/CPF)**

---

**TRANSACTION MONITORING, SCREENING AND SUSPICIOUS ACTIVITY  
REPORTING GUIDELINES**

**2024**

## Table of Contents

ACRONYMS AND ABBREVIATIONS.....	2
DEFINITIONS.....	3
1. SCOPE AND APPLICATION OF THE GUIDELINES.....	4
2. TRANSACTION MONITORING .....	4
A. AML/CFT/CPF Transaction Monitoring Process .....	5
B. Transaction Monitoring Methods .....	6
C. Risk Signals when Evaluating Transactions for Suspicious Activity.....	7
3. TARGETED FINANCIAL SANCTIONS (TFS) SCREENING.....	7
A. Steps to follow when manually screening against the UNSC Consolidated List.....	8
4. SUSPICIOUS TRANSACTION REPORTS .....	11
A. The Legal Obligation to submit an STR.....	12
B. How to Identify a Suspicious Transaction or Activity .....	12
C. How to register on the GoAML Platform .....	13
D. How to Submit a STR .....	13
5. CASH TRANSACTION REPORTS (CTRs).....	13
6. COMMENTS.....	14
7. REFERENCES .....	14
8. ANNEXURES.....	14

## ACRONYMS AND ABBREVIATIONS

<b>AML/CFT/CPF</b>	Anti-Money Laundering, Combating Financing of Terrorism and Countering Proliferation Financing
<b>CDD</b>	Customer Due Diligence
<b>CTR</b>	Cash Transaction Report
<b>FATF</b>	Financial Action Task Force
<b>FIU</b>	Financial Intelligence Unit
<b>ML/TF/PF</b>	Money Laundering, Terrorism Financing and Proliferation Financing
<b>MLPCA</b>	Money Laundering and Proceeds of Crime Act
<b>SECZim</b>	Securities and Exchange Commission of Zimbabwe
<b>SIMs</b>	Securities Market Intermediaries
<b>STR</b>	Suspicious Transaction Report
<b>TFS</b>	Targeted Financial Sanctions
<b>UN</b>	United Nations
<b>UNSCRs</b>	United Nations Security Council Resolutions

## DEFINITIONS

For purposes of these Guidelines:

**Cash** - implies coin and paper money of Zimbabwe or of another country, which is designated as legal tender and circulates as, and is generally used and accepted as, a medium of exchange in Zimbabwe or the country of issue.

**Cash transaction** - The Financial Action Task Force (FATF) defines a cash transaction as any financial activity involving physical currency (coins or notes).

**Cash transaction reports** – are reports submitted after tracking large cash transactions and movements that exceed the FIU Threshold Directive for the specified period.

**Financial Intelligence Unit** – means the Unit defined in section 6A of the Money laundering and Proceeds of Crime Act [Chapter 9:24].

**Securities Market Intermediaries** - refers to persons licensed in terms of section 38 of the Securities and Exchange Act [Chapter 24:25].

**Suspicious transaction report** - means a report required to be made under section 30 Money laundering and Proceeds of Crime Act [Chapter 9:24].

**Transaction** – has a definition on section 13 of Money laundering and Proceeds of Crime Act [Chapter 9:24].

**Transaction Monitoring** - A process of reviewing and comparing customer transactions to customer risk profiles and typical transaction patterns. Subsequently, conducting a focused examination of transactions and identifying possible suspicious transactions.

## **1. SCOPE AND APPLICATION OF THE GUIDELINES**

- 1.1 These guidelines aim to clarify and provide practical assistance to securities market intermediaries (SMIs) in identifying suspicious transactions and meeting their reporting obligations under section 30 of the Money Laundering and Proceeds of Crime Act (MLPCA). [Chapter 9:24].
- 1.2 These guidelines set out the reporting requirements and procedures for submitting Suspicious Transaction Reports (STRs) and Cash Transaction Report (CTRs) to the Financial Intelligence Unit. Specifically, it explains transaction monitoring, screening, reporting, reporting timelines, the information that must be included when reporting, and the procedure for reporting to the FIU using the goAML platform.
- 1.3 The Securities and Exchange Commission of Zimbabwe (SECZim) emphasizes that the contents of these guidelines are only intended to provide general information and guidance and do not encompass all of the law's requirements. It is also not intended to replace the reader's own assessment, nor to absolve the user of this guideline from their responsibility to exercise their own skill, knowledge, and due care in relation to the specific circumstances of the transaction/activity.
- 1.4 These guidelines are not intended to constitute legal advice from the Commission or to replace the MLPCA.

## **2. TRANSACTION MONITORING**

- 2.1 SMIs should closely examine their customers' transactions to ensure they align with their understanding of their commercial or personal activities, as well as their risk profile. Transaction monitoring processes or systems may vary in scope or sophistication (e.g., using manual spreadsheets and exception reports to automated and complex systems or a combination of both) depending on the size, volumes and complexity of the business operations. Since transactions will not all be suspicious, SMIs should also have processes to analyse transactions, patterns and activity to determine if they are suspicious and meet the reporting threshold.

- 2.2 SMIs should pay attention to the following while conducting their transaction monitoring activities:
- 2.2.1 size, frequency, or patterns of transactions that may indicate unusual or suspicious activity, such as suspected fraud or identity theft;
  - 2.2.2 transactions that are sent to or received from a high-risk country or region;
  - 2.2.3 payments that are sent to or received from a person or organisation on a sanctions list;
  - 2.2.4 activities that may be inconsistent with a customer's risk profile or history;
  - 2.2.5 activities of higher risk customers previously suspected of or investigated for potentially suspicious activity; and
  - 2.2.6 other unexpected account activity from a customer which may indicate money laundering or terrorism financing.
- 2.3 The Compliance or Money Laundering Reporting Officer should document transaction monitoring findings and keep records for at least five years. The findings should be made available immediately if requested by the FIU, the Commission, a local or foreign counterpart supervisory authority, or any other authority prescribed by the responsible Minister.

#### **A. AML/CFT/CPF Transaction Monitoring Process**

- 2.4 **Customer identification.** It entails identifying and verifying customer information such as name, address, and identification documents. Customer identification is critical for monitoring transactions and detecting suspicious behavior.
- 2.5 **Setting alerts.** This entails the generation of alerts based on predetermined criteria. Alerts can be tailored to the needs of each SMI and can include criteria such as unusual transaction patterns, high-risk customers, or known money laundering typologies.
- 2.6 **Identification of suspicious behavior.** SMIs should classify suspicious behaviors and establish parameters for detecting potentially illegal

activities. This can be done based on transactions volume, frequency, or geographical location. The system must also be able to adapt to new and emerging risks, such as changes in regulatory requirements or sanctions.

- 2.7 **Transaction analysis.** It entails analysing individual transactions, including their amount, origin, and destination. Transaction analysis assists in identifying potentially suspicious activity and detects money laundering and other financial crimes.
- 2.8 **Investigation and Escalation.** When potentially suspicious activity is detected, it should be investigated and reported to the proper authorities. This involves the SMI compliance team filing a STR that can be processed by the FIU and work with law enforcement agents if a case is to be pursued.
- 2.9 **Reporting.** As required by law, SMIs must report suspicious activity or transaction to the FIU through goAML. Failure to do this may result in severe financial penalties and reputational damage.
- 2.10 **Review.** This includes reviewing the parameters and alerts to ensure they are still relevant and useful, as well as reviewing any false positives or negatives to identify areas for improvement.
- 2.11 **Audits.** SMIs must provide a clear audit trail for monitoring and investigations. This helps to demonstrate compliance with regulatory requirements and identify potential gaps in the transaction monitoring process. Monitoring reports should be drafted and kept for at least five years after the date of monitoring.

## **B. Transaction Monitoring Methods**

- 2.12 **Manual transaction monitoring.** This is where a team of analysts, or a compliance officer/money laundering reporting officer, reviews transactions to determine whether they are suspicious or not. This approach can be time-consuming and expensive for larger SMIs with significant number of transactions, but it can be effective for smaller SMIs. A Trustee may also perform this function to ensure that trust funds are not abused by managers.

2.13 **Automated AML transaction monitoring.** This is a software that is used to review transactions and identify any transactions that appear suspicious. This approach is faster and more efficient than manual monitoring, and when combined with artificial intelligence, automation can provide a comprehensive view of customer behaviour, including detailed transaction logs. However, automation does not replace the human eyes and thought processes that are necessary to fully understand potential ML/TF/PF risk.

### **C. Risk Signals when Evaluating Transactions for Suspicious Activity**

2.14 **Geography:** Where is the transaction being initiated? Where is it being completed? Are any of these locations in a high-risk country or jurisdiction, as defined by the Financial Action Task Force (FATF) or other regulators?

2.15 **Amount:** How big is the transaction? For example, does it appear that the customer is making one or multiple transactions just below the threshold—a process known as structuring, or smurfing?

2.16 **Velocity:** Have customers significantly increased their spending or transaction volume compared to their average activity (for example, daily or weekly averages)? Has the customer initiated a large number of transactions in a short period of time, such as in the last 30 minutes?

2.17 **Recipient:** Has the customer initiated or attempted a transaction in which the recipient is deemed high risk? For example, a known bad actor, that is for instance someone with adverse media, someone on a watchlist or sanctions list, or a politically exposed person.

2.18 **Annexure 1** outlines the transaction monitoring key red flags.

## **3. TARGETED FINANCIAL SANCTIONS (TFS) SCREENING**

3.1 TFS are sanctions imposed through United Nations Security Council Resolutions (UNSCRs) against specific individuals and entities identified by



the United Nations (UN) Security Council (or relevant UN committees) as contributing to a particular threat to, or breach of, international peace and security.

- 3.2 Zimbabwe, as a member of the UN, has committed to implementing the UNSCRs through legislation, including the Suppression of Foreign and International Terrorism Act [Chapter 11:21] and relevant Statutory Instruments.
- 3.3 To implement TFS, SMIs must screen their clients against the UNSC Consolidated List, immediately (i.e. without delay and not later than 24 hours) after receiving the Directive from FIU, verify the details of the Listed Party with their client books. If there is a positive match, they should immediately file an STR with the FIU. SMIs are also required to visit UN website and watchlists for their screening purposes.
- 3.4 SMIs are required to conduct screening when onboarding customers, and throughout the life cycle of the customer relationship. The screening should also include directors and beneficial owners of corporate customers or legal arrangements. Screening should also be done at regular intervals either upon a trigger event or when a sanctions list changes. SMIs should also screen before hiring new employees. This can prevent trading with sanctioned entities and protect the workplace.
- 3.5 The data screened against must be comprehensive and high-quality. Do not just rely on search engines. You will need to enlist a network of experts around the globe that are multilingual and collating data 24/7. Watchlists that are consolidated in one place in a database can be helpful.

## **A. Steps to follow when manually screening against the UNSC Consolidated List**

### **Step 1 - Open the UNSC Consolidated List.**

- (a) Access the UNSC Consolidated list webpage on the link:  
[<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>]

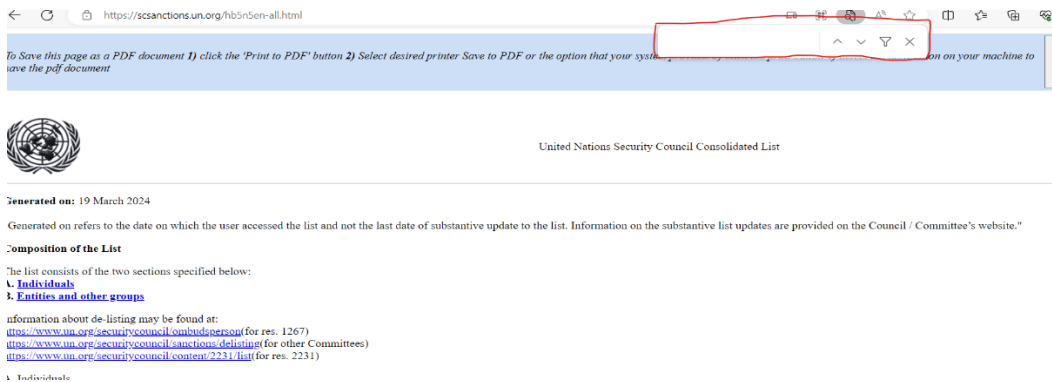


(b) Select the PDF version as indicated by the arrow below to access the UNSC Consolidated list.

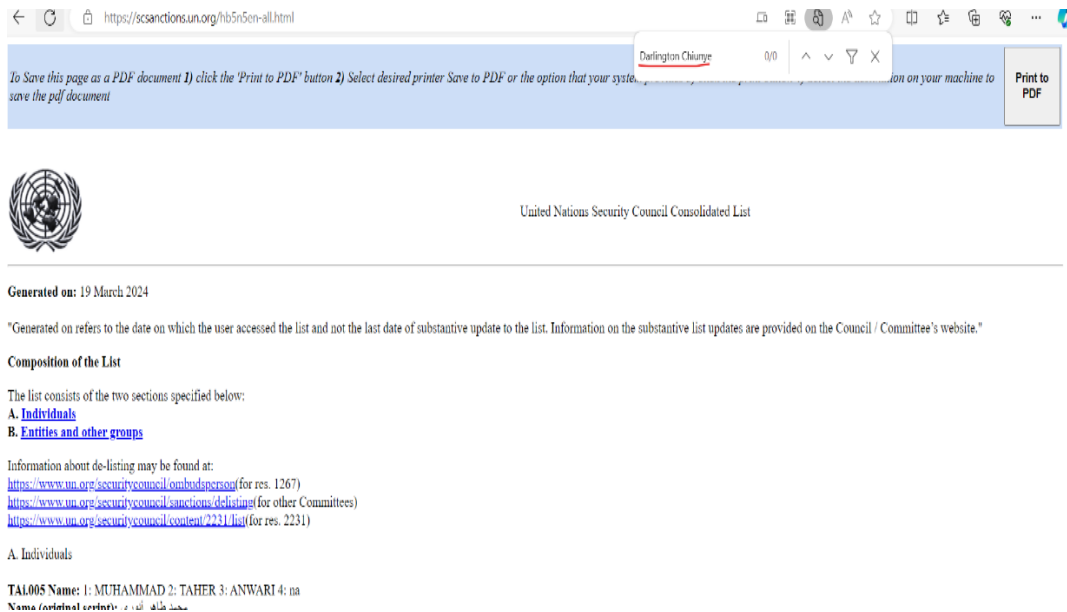


**Step 2 - Search ('screen') your client for a match on the UNSC Consolidated List.**

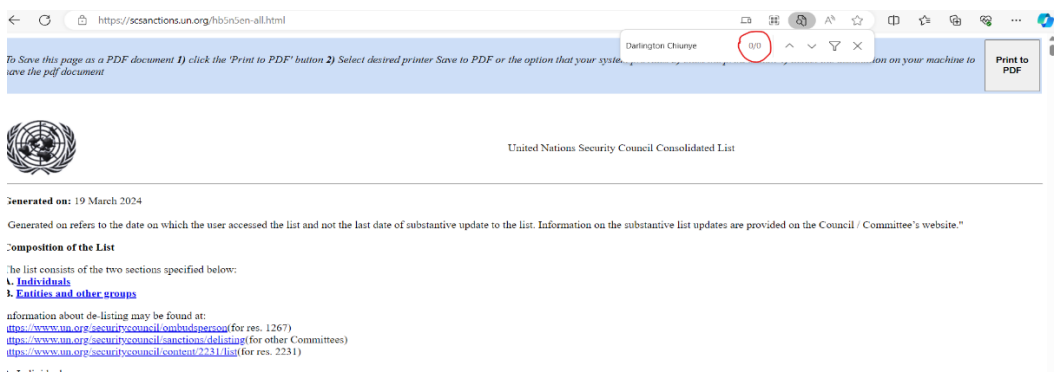
(a) Once the list is open, on your keyboard, press Ctrl + F to open the Find field.



(b) Type your search name (client name, for example Darlington Chiunye) in the Find field.



(c) The screening results will be indicated in the Find field as below:



- The screening results above show no match to the UNSC Consolidated list i.e., 0 results.

### Step 3 - Keep record of the TFS screening done & the results

- Take a screenshot of your screen shown in the visual.
- Save the screenshot on a word document. You may save it electronically or in hard copy as per your record keeping policy as part of client CDD.



## Step 4 - If match found, proceed with reporting to FIU

If the client's name appears on the UNSC Consolidated list, it implies that the client is a true match:

- (a) When a true match with a listed/designated person is identified by an SMI, it should be reported immediately to the FIU via goAML platform.

## 4. SUSPICIOUS TRANSACTION REPORTS

- 4.1 If an SMI suspects or has reasonable grounds to suspect that the funds are the proceeds of a criminal activity, or related or linked to terrorist financing, they should promptly (within three working days after forming the suspicion) report their suspicions to the FIU.
- 4.2 All STRs should be reported to FIU regardless of the amount involved in the transaction.
- 4.3 SMIs, their directors, officers, and employees (permanent and temporary) are protected by law from both criminal and civil liability, if they report their suspicions in good faith to the FIU (see section 32 of MLPCA). The FIU has mechanisms to ensure that names and personal details of the staff of the SMIs that made the STR are kept confidential.
- 4.4 SMIs, their directors, officers, and employees are prohibited by law from disclosing (tipping off) the fact that an STR or other related information is being reported to the FIU (see section 31 of MLPCA); otherwise, it may prejudice the future investigation carried on by the FIU. However, sometimes a risk exists that customers may be unintentionally tipped off when an SMI is seeking to perform its CDD measures; therefore, the

institution and their employees should be aware of and adequately trained on how to efficiently handle these sensitive issues when conducting CDD measures.

## **A. The Legal Obligation to submit an STR**

- 4.5 A SMI must submit an STR to the FIU if a transaction or activity has been conducted or attempted by or through its institution and it knows or suspects that the transaction or activity may relate to ML/TF/PF activities or other financial crimes. The requirement to report suspicious transactions applies to all types of transactions.
- 4.6 The obligation to report an STR is in terms of section 30 (1) of MLPCA.

## **B. How to Identify a Suspicious Transaction or Activity**

- 4.7 SMIs must develop their own understanding of reasonable suspicion which may be related to risk indicators and incorporate established views of doubt about circumstances relating to the behaviour, to a transaction, to a series of transactions, an attempted transaction or to any combination thereof.
- 4.8 A number of indicators, as listed in the **annexure 2**, can assist in identifying or recognising a suspicious transaction or activity in the securities sector. However, indicators alone do not confirm a ML/TF/PF offence or criminal conduct. An assessment of the suspicion should be based on a reasonable evaluation of other relevant factors, including the knowledge of the customer's business, financial history, background and behaviour.
- 4.9 An SMI should know its customers and understand their line of business. Transactions or activities that are not within the normal practices of their customer's line of business could then be identified and used to determine whether there are reasonable grounds to suspect that the transactions or activities are related to ML, TF or PF.

## C. How to register on the GoAML Platform

4.10 All SMIs must be registered on the goAML platform to enable them to submit their STRs to the FIU. To register on goAML platform, the SMI should follow the process outlined on **annexure 3**.

## D. How to Submit a STR

4.11 When the registration on the goAML platform is successfully completed, the SMI will be able to submit their STRs to the FIU electronically. To complete the reporting obligations, SMIs should follow the steps outlined on **annexure 4**.

## 5. CASH TRANSACTION REPORTS (CTRs)

5.1 All transactions completed by or on behalf of a customer in cash (received and paid) above the threshold as updated by the FIU on a regular basis must be reported to the FIU. SMIs must record large cash transactions, and reports must be submitted electronically via the goAML platform.

### The reportable transactions must be limited to:

- (i) Cash collected or cash paid by the SMIs at its premises above the prevailing threshold; and
- (ii) Cash deposit directly into the SMIs Bank Account above the prevailing threshold.

5.2 All SMIs are required to submit CTR returns. These reports should be submitted to the FIU monthly. The returns, **including nil returns**, should be submitted on or before the 10<sup>th</sup> day of every month.

5.3 The FIU from time-to-time issues threshold directives in terms of section 30(5) and (6) of MLPCA with revised thresholds for CTRs and all SMIs are required to comply with those directives as they are issued by the FIU.

## **Therefore:**

- (i) The SMIs should review their internal records for cash received and/or paid (above threshold) at the business premises as from 10<sup>th</sup> September 2024; and
- (ii) Review the Bank Statements for cash deposits and/or cash payments above threshold as from 10<sup>th</sup> September 2024.

## **6. COMMENTS**

- 6.1 This Guidelines shall be reviewed from time to time depending on the global developments in the fight against Money Laundering, the Financing of Terrorism and Proliferation Activities.

## **7. REFERENCES**

FATF (2018), *Guidance for a Risk-Based Approach for the Securities Sector*, FATF, Paris, [www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-securities-sector.html)

FATF and MENAFATF (2015), *Money Laundering through the Physical Transportation of Cash*, FATF, Paris, France and MENAFATF, Manama, Bahrain, [www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html](http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html)

Money Laundering and Proceeds of Crime Act [Chapter 9:24].

Suppression of Foreign and International Terrorism Act [Chapter 11:21]

Securities and Exchange Act [Chapter 24:25].

## **8. ANNEXURES**

### **Annexure 1: Transaction Monitoring Key Red-Flags**

- Customer, who is a student uncharacteristically transfers or exchanges huge sums of money.
- Transactions involve offshore institutions whose names resemble those of well-known legitimate financial institutions.

- The customer, who is a public official, opens an account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income.
- Transaction involves offshore countries or tax haven countries like British Virgin Island, Bahama Island, and Cooks Island.
- Transaction that involves depositing a large amount of cash inconsistent with the normal and expected activity of the customer.
- Accounts show high velocity in the movement of funds but maintain low beginning and ending daily balances.

## **Annexure 2 . Suspicious Activity Indicators in Relation to Securities**

### **I. Product/Customer transactions suspicious activity indicators**

1. Transactions do not have apparent economic rationale.
2. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/reporting thresholds.
3. A concentration ratio of transactions relating to a particular and/or higher risk jurisdiction that is notably higher than what is to be expected considering its normal patterns of trading of a customer.
4. Frequent trades resulting in losses for which the customer appears to have no concern.
5. Sudden spike in transaction volumes, which deviates from previous transactional activity absent any commercial rationale or related corporate action event.
6. Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes.
7. A pattern of securities transactions indicating the customer is using securities trades to engage in currency conversion.
8. Trading in the same security or securities between numerous accounts controlled by the same people (e.g., potential wash sales and/or directed trading).
9. Two or more unrelated accounts at the securities dealing firm trade an illiquid or low-priced security suddenly and simultaneously.
10. Transactions that suggest the customer is acting on behalf of third parties with no apparent business or lawful purpose.
11. Funds deposited for purchase of a long-term investment followed shortly by a customer request to liquidate the position and transfer the proceeds out of the account.



## **II. Distribution channel suspicious activity indicators**

1. Intermediaries whose transaction volume is inconsistent with past transaction volume absent any commercial rationale or related corporate action event.
2. A transaction pattern indicating a value of transactions just beneath any applicable reporting threshold.
3. Unclear or complex distribution channels that might limit the ability of the investment fund or asset management company to monitor the transactions (e.g. use of a large number of sub-distributors for distributions in other countries).

## **III. Selected indicators of suspicious trading or market manipulation**

1. Making a large purchase or sale of a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation.
2. A request is made to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
3. Accumulation of stock in small increments throughout the trading day to increase price.
4. Engaging in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
5. Marking the closing price of a security.
6. Front-running suspected with regard to other pending customer orders.

## **IV. Suspicious indicators associated with CDD and interactions with customers**

1. Customer's legal address is associated with other, apparently unrelated, accounts. Locations of address of the customer, bank or financial institution seem unconnected to the customer and little or no explanation can be given by the customer for the disparate addresses.
2. Customer is a trust, or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
3. Customer is publicly known to have criminal, civil or regulatory proceedings against it for corruption, misuse of public funds, other financial crimes or regulatory non-compliance, or is known to associate with such persons. Sources for this information include news items or Internet searches.

4. Customer's background is questionable or differs from expectations based on business activities.
5. Customer has been rejected or has had its relationship terminated as a customer by other SMIs or financial institution.
6. Customer's account information reflects liquid and total net worth that does not support substantial account activity.
7. Customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
8. Non-profit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
9. Customer is reluctant to provide information in relation to its identity and/or transactions.
10. Customer is reluctant to provide information needed to file reports to proceed with the transaction or requests an inordinate amount of secrecy around a transaction.
11. Customer exhibits unusual concern with the firm's compliance with government reporting requirements, the firm's systems or the firm's AML/CFT/CPF policies and controls.
12. Customer tries to persuade an employee not to file required reports or not to maintain the firm's required records.
13. Law enforcement or other supervisors have issued freeze letters regarding a customer and/or account at the securities firm.
14. Customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy.
15. Customer does not exhibit a concern with the cost of transactions or fees (e.g. surrender fees, higher than necessary commissions) or of investment losses.

**V. Suspicious indicators in deposits of securities, particularly low-priced securities; these can often be indicators of low-priced securities fraud, distribution of an unregistered offering, or market manipulation schemes.**

1. A sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
2. The lack of a restrictive legend on shares physically or electronically deposited seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock, and/or the volume of shares trading.
3. Customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange listed securities.
4. Customer's explanation of how the customer acquired the securities does not make sense or changes.
5. Customer deposits physical securities or delivers in shares electronically and requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

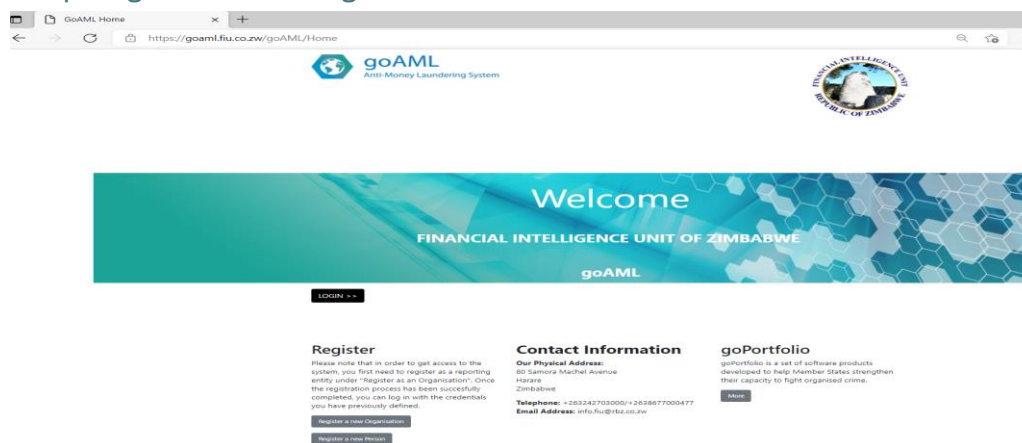
#### **VI. Movement of funds or securities**

1. The securities account is used for payments or outgoing wire transfers with little or no securities activities (i.e. account appears to be used as a depository account or a conduit for transfers with no reasonable business explanation for such).
2. Customer "structures" deposits, withdrawals or purchase of securities below a certain amount to avoid reporting or recordkeeping requirements.
3. Customer engages in excessive journal entries of funds or securities between related or unrelated accounts without any apparent business purpose. Payment by third parties from a source that has no apparent connection to the customer.
4. Customer uses a personal/individual account for business purposes.
5. Payment to a third party to which the customer has no apparent connection.
6. Frequent transactions involving round or whole dollar amounts.
7. Funds transferred into an account that are subsequently transferred out of the account in the same or nearly the same amounts, especially when origin and destination locations are high-risk jurisdictions.
8. A dormant account suddenly becomes active without a plausible explanation (e.g. large amounts are suddenly wired out).
9. Transfers of funds or securities are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.

10. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
11. Customer transfers/receives funds to/from persons involved in criminal or suspicious activities (as per the information available).
12. In/out transactions for substantial amounts on a short-term basis.
13. Receipt of unexplained amounts, followed, shortly thereafter, by a request to return amounts.
14. Frequent transfers of securities' ownership.
15. Frequent change of bank account details or information for redemption proceeds, in particular when followed by redemption requests.

### Annexure 3: How to register on the GoAML Platform

1. To access the GoAML Homepage, click on the GoAML: <https://goaml.fiu.co.zw/goAML/Home>



2. Go on Register Business Registration Details (Fields with an asterisk (\*) are mandatory fields)

3. Business Contact Details (Fields with an asterisk (\*) are mandatory fields)

Contact Type	Comm. Type	Country Prefix	Number
Business	Mobile Phone	+263	0777111000

<b>Phone</b>			
Contact Type™	Business	Comm. Type™	Mobile Phone
Country Prefix	+263	Number™	0777111000
Extension		Comments	
<input type="button" value="Add"/>		<input type="button" value="Cancel"/>	

Address	City	State	Zip	Country
100 First Street	Harare	Harare	0000	ZIMBABWE

<b>Address</b>			
Type™	Business	Address™	100 First Street
Town	Harare	City™	Harare
Zip	0000	Country™	ZIMBABWE
State	Harare	Comments	
<input type="button" value="Add"/>		<input type="button" value="Cancel"/>	

4. Compliance Officer/MLRO Contact Details - This section requires information of the MLRO (Money Laundering Reporting Officer) of the organization.

<b>Registering Person</b>			
User Name™	Johnny	Email™	johnndoe@abcaccountants.co.zw
Password™	.....	Confirm Password™	.....
Gender	Male	Title	Mr
First Name™	John	Last Name™	Doe
Birth Date	01/01/1985	NRSA Number	111111
Nationality	ZIMBABWE	Occupation™	Accountant
National ID	12-3456789-A-00		
Passport?	<input checked="" type="radio"/> No <input type="radio"/> Yes		

Contact Type	Comm. Type	Country Prefix	Number
Private	Mobile Phone	+263	0777000000

<b>Phone</b>			
Contact Type™	Private	Comm. Type™	Mobile Phone
Country Prefix	+263	Number™	0777000000
Extension		Comments	
<input type="button" value="Add"/>		<input type="button" value="Cancel"/>	

5. Business Address - Once all the information has been filled in, submit the request.

Address	City	State	Zip	Country
200 Seventh Street	Harare			ZIMBABWE


  

<b>Address</b>			
Type™	Private	Address™	200 Seventh Street
Town	Harare	City™	Harare
Zip		Country™	ZIMBABWE
State		Comments	
<input type="button" value="Add"/>		<input type="button" value="Cancel"/>	

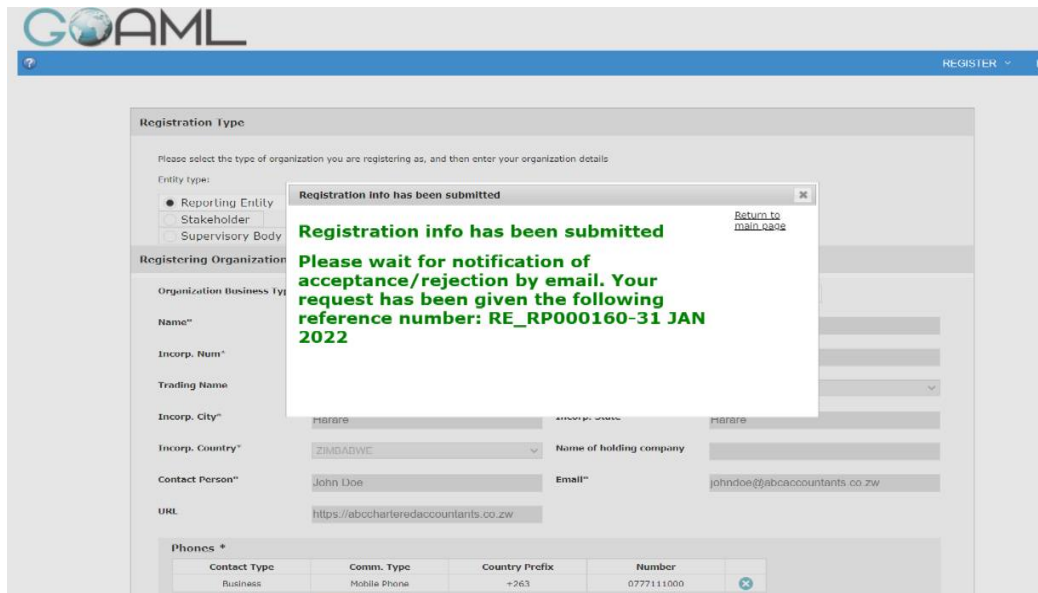
  

<b>Attachments</b>	
File Name	File Size
<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Upload"/>	

075333	
<input type="button" value="Submit Request"/>	

6. Registration Successful



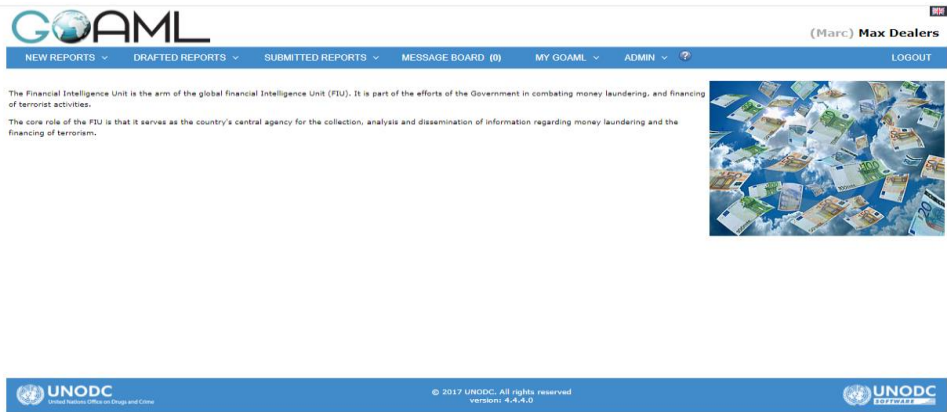
#### Annexure 4: Reporting Details

The goAML Web application (goAML Web) is not freely accessible, you must have special access permissions (credentials) to be able to work with it. You should enter <https://goaml.fiu.co.zw/goAML/Home> for the production environment, the goAML Home Page is launched.

1. Click on Login on the top-left side highlighted in black colour then login using your user credentials.



2. Results after login - the application's home page is loaded and displayed

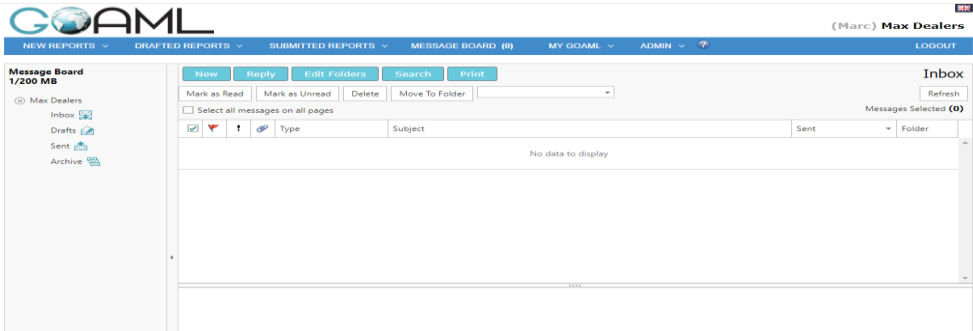


## The goAML WEB user interface

- (a) **Message Board:** The goAML message board is the internal means of communication between goAML users. The intention is to connect the users of the goAML application with the reporting entities and stakeholders using the goAML Web Portal. The message board is organized like an email client. messages can only be sent from the users to the Financial Investigation Unit they report to and vice versa. There are no individual message boxes.
- (b) **New Reports:** One of the main reasons for working with goAML Web is submitting financial reports to the goAML system. Reports can either be uploaded as XMLs files or Web reports.

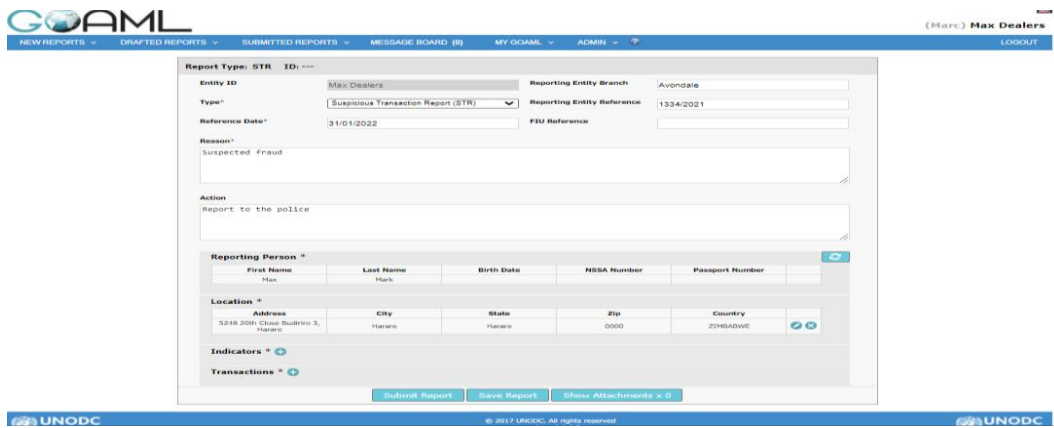
### Report Indicators:

- (a) To add certain report indicators (e.g. Cash deposits, fraud) select from the indicators grid. You can choose the relevant code/indicator and select the checkbox next to it. You can choose more than one report indicator.
  - (b) To remove a report indicator, select it in the list and click on √.
  - (c) As there is no special report category for terrorism financing reports, make sure that in case of suspicious activity or suspicious transaction involving terrorist financing, at least the indicator “Terrorism financing” is selected.
3. Select Message Board from the menu bar. The goAML message board is loaded and the inbox displayed:

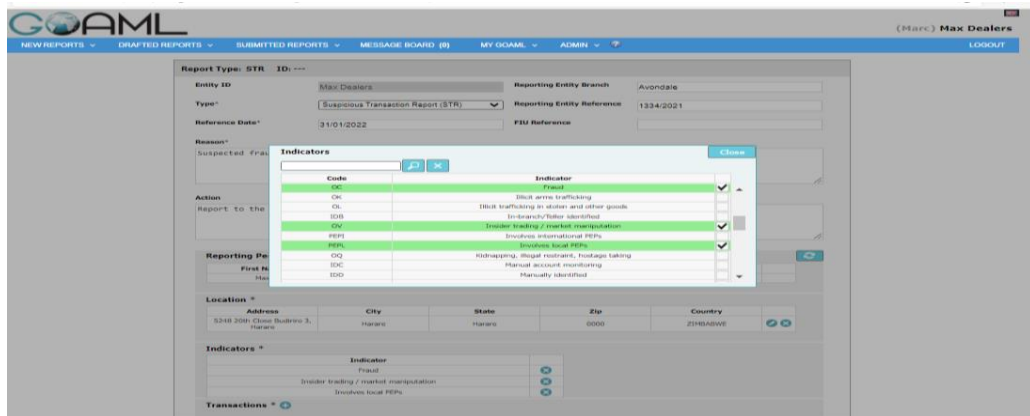


- Transaction: Click on to add Transactions to the Web Report, fill in all the relevant transaction details on the Transaction form, and Click on Add Transaction and Save Report.

### Web reports



### Indicators



What does the transaction section look like?



All the Transactions that have been added and saved appear in the transactions grid as shown below.

#	Number	Date	Local Amount	Transmode Code	Status	
1	TRNWEB0286 02 OCT 13	10/03/2013	3000000	Electronic transaction	Require at least one party	
2	TRNWEB0290 02 OCT 13	10/02/2013	90000	ATM	Missing From Party	
3	TRNWEB0291 02 OCT 13	10/17/2013	348989434890890234	Electronic transaction	Require at least one party	

### Involved Parties:

For every submitted transaction, the involved parties have to be defined.

- (a) Select one of the checkboxes for Party is : My Client or Not My Client as the case maybe.
- (b) Select the Party Type checkbox : Person, Account or Entity.
- (c) Depending on the Party Type selection, the corresponding form for the details will open up.
- (d) Enter the details for the involved party (fields marked with an asterisk are mandatory):
  - (i) Funds Code: Select a type of funds from the drop-down menu provided i.e. cash, cheque etc.
  - (ii) Funds Comment: If you want, add a comment about the type of funds transferred.
  - (iii) Country: Select the country of this transaction party.

- (iv) **Foreign Currency:** Click on the icon to open up the Foreign Currency window.

The results are shown below:

**From Party**

Funds Code\*  Funds Comment

Country\*

Foreign Currency +

Conductor +

Party Type:\*  Person  Account  Entity

Add Party and Save Report Cancel

**Foreign Currency:**

- (a) **Currency Code:** The currency in which the transaction was at this state. Select one from the drop-down list.
- (b) **Amount:** The amount of the transaction in the foreign currency.
- (c) **Exchange rate:** The exchange rate between the foreign currency and the default currency of the FIU’s country.

**Foreign Currency**

Currency Code\*  Amount\*

Exchange Rate\*

Save Cancel

**Conductor:**

If the transaction party is a person, click on the icon to open up the Conductor window as shown below:

The screenshot shows a 'Person' form with the following fields and values:

- Title: Mr
- First Name: Peter
- Second Name: (empty)
- Birth Date: (empty)
- Mother's Name: (empty)
- PKNA Number: (empty)
- Nationality 1: BANGLADESH
- Nationality 2: (empty)
- Occupation: (empty)
- Driver's License: (empty)
- Source of Wealth: (empty)
- Passport?  NO  YES
- Deceased?  NO  YES
- Gender: Male
- Last Name: Younger
- Resident Name: (empty)
- Birth Place: (empty)
- Alias: (empty)
- National ID: 32-112340N32
- Residence: (empty)
- Employer Name: (empty)
- EC Number: (empty)

Below the main form are sections for 'Phones', 'Addresses', 'Identification', 'Emails', 'Employer Address', and 'Employer Phone', each with a plus icon to expand. A 'Comments' text area is at the bottom. 'Save' and 'Cancel' buttons are at the bottom right.

If you have an identity document of the person, click on the icon to add an Identification.

The screenshot shows an 'Identification' form with the following fields:

- Type\*: (empty dropdown)
- Number\*: (empty text box)
- Issue Date: (empty text box)
- Expiry Date: (empty text box)
- Issued by: (empty text box)
- Issue Country\*: BANGLADESH (dropdown)
- Comments: (empty text box)

'Save' and 'Cancel' buttons are at the bottom right.

- (a) Type : Select the type of document from the drop-down list (e.g. a passport).
- (b) Number : The identification number of the document.
- (c) Issue Date : Enter the issue date of the document into the field or select it using the calendar pop-up (calendar icon).
- (d) Expiry Date: The last date of validity of this document.
- (e) Issue Country: Select the country issuing the document.

If you know the address of the person, click on icon to unfold this section of the window. Fill in the mandatory fields with the address details as requested below.

The screenshot shows an 'Address' form with the following fields:

- Type\*: (empty dropdown)
- Address\*: (empty text box)
- Town: (empty text box)
- City\*: (empty text box)
- Zip: (empty text box)
- Country\*: BANGLADESH (dropdown)
- State: (empty text box)
- Comments: (empty text box)

'Save' and 'Cancel' buttons are at the bottom right.

### Goods and Services:

- (a) If the transaction includes items of any kind, then these items have to be defined here as well.

(b) In the transaction window, click on the icon for Transaction items. An input window is shown below:

Transaction Item			
Item Type*	<input type="text"/>	Item Make	<input type="text"/>
Description	<input type="text"/>	Previously Registered To	<input type="text"/>
Presently Registered To	<input type="text"/>	Estimated Value	<input type="text"/>
Status Code	<input type="text"/>	Disposed Value	<input type="text"/>
Currency Code	<input type="text"/>	Size	<input type="text"/>
Size UOM	<input type="text"/>	Registration Date	<input type="text"/>
Registration Number	<input type="text"/>	Identification Number	<input type="text"/>
Comments	<input type="text"/>		
<b>Address</b>			
Status Comments <input type="text"/>			
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>	

## 5. Submit Report:

- (a) After you have completed the Web Report, added all the transactions, the transaction parties and items associated with the transactions, you can save all the details and preview it before clicking on the Submit button.
- (b) Click on the Submit Report link. After a security check, the report is added to the submitted reports in the goAML Web database.
- (c) **Drafted Reports:** The Drafted Reports menu allows you quick access to the report you are currently working on and a list of all Not Submitted Web Reports
- (d) **Submitted Reports:** Every user can view his or her already submitted reports in their current state. goAML Web separates them into two lists containing uploaded XML reports and manually created Web Reports respectively.



---

A. Taruvinga  
**Chief Executive Officer**