FINANCIAL
INTELLIGENCE UNIT

REPUBLIC OF MAURITIUS

AML/CFT insights

October - December 2019

Issue no. 3 / 09 March 2020

About the Financial Intelligence Unit

In 2002, the Financial Intelligence Unit (FIU) was set up under the Financial Intelligence and Anti Money Laundering Act 2002 (FIAMLA) to operate as an independent central agency, having the core functions of, (a) receiving information concerning suspected proceeds of crime and alleged money laundering offence through Suspicious Transactions Reports (STRs) and non-STR disclosures; (b) collecting information, carrying out financial investigative analysis and; (c) where appropriate, making disseminations to investigatory and supervisory authorities and Registrars concerning suspected proceeds of crime, alleged money laundering offences and the financing of any activities or transactions related to terrorism. The products of the FIU are intelligence packages that constitute leads for use by investigatory and supervisory authorities in carrying out their functions. The department dealing with the core functions of the FIU is known as the Financial Investigative Analysis Division (FIAD).

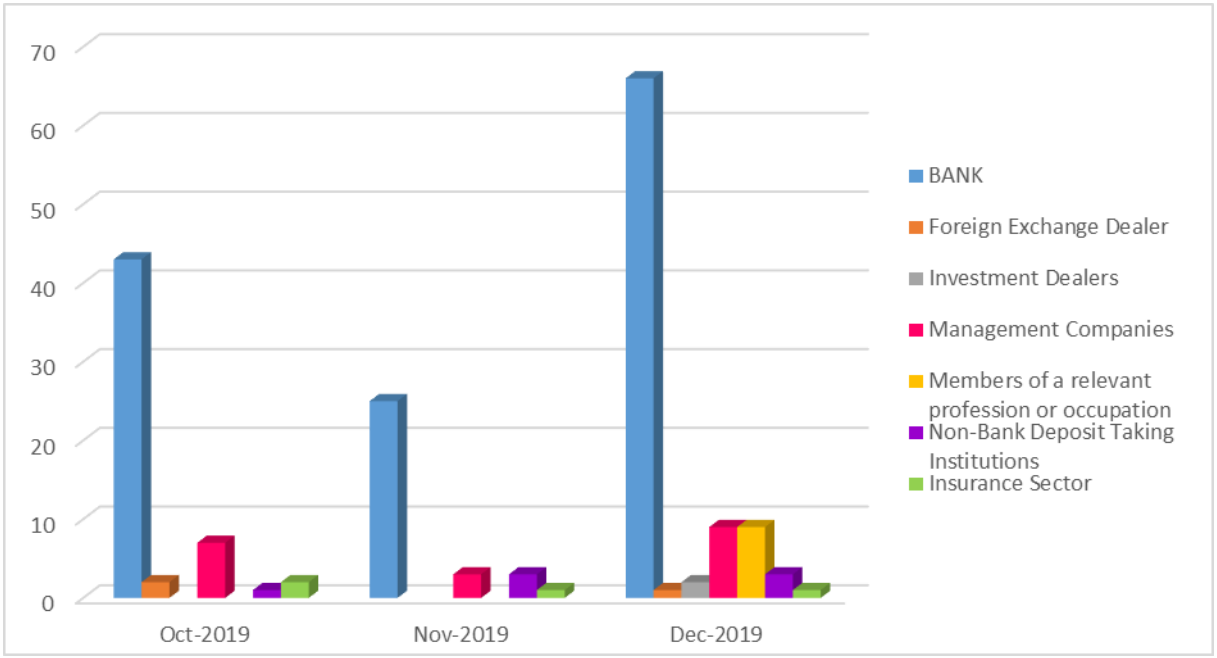
About this publication

The main objectives of this publication are to provide quarterly insights into the STR reporting trends in Mauritius, as well as highlights of new developments in AML/CFT. This publication will also be one of the means through which the FIU fulfils its obligations under Section 14(1A) of FIAMLA to provide regular feedback to reporting persons and relevant supervisory authorities.

Table of Contents

Number of STRs filed to the FIU

During the period from 01 October 2019 to 31 December 2019, a total of 178 STRs were reported to the FIU, with banks being the main STR provider with about 75% of STRs filed. Comparatively, for the last period surveyed (01 July 2019 to 30 September 2019), banks had filed about 80% of STRs. This percentage decrease confirms the trend already observed during the last quarter surveyed, namely the emergence of a shift in the composition of STR providers, especially as observed for the month of December 2019. And although the number of STRs filed during the current quarter has experienced a decrease of about 28% compared to the last quarter, it is worthwhile to note that the aggregate value of transactions reported in the current quarter account for 34 times more than aggregate value of the past quarter; this is dealt in more details in the next section of this bulletin.



Out of the 178 STRs, 169 were filed via the goAML application and 9 were filed via paper submissions.

STRs from Gambling sector

The paper submissions were effected by Members of relevant profession or occupation from the Gambling sector. The trend in STR reporting for this sector continues to be steady this quarter, showing a welcome improvement in the awareness of reporting persons of their AML/CFT obligations in that sector. Yet, it continues to be alarming that in reports received, the same patterns of suspicious transactions were observed, namely the fact that reporting persons were unable to obtain identification from their customers who engaged

STRs from Gambling sector (continued)

into business relationships, involving cash transactions, with them. In some instances, the customers had only nominally exchanged cash for tokens to only later cash out the tokens without performing any gambling operations.

Clearly, the easy anonymity afforded when engaging in business transactions in the Gambling sector poses a heightened money laundering risk and renders the work of the FIU, supervisory and investigatory bodies more arduous in identifying suspects, linkages and money laundering schemes. Thus, there is clearly much room to strengthen the supervisory, regulatory and compliance framework in the Gambling sector in terms of CDD measures, customer acceptance policies and procedures and record keeping.

STRs from Insurance Sector

Comparing the current quarter to the last, the number of STRs reported by the Insurance Sector experienced a twofold increase. In general, money laundering risks associated with the Insurance sector are considered to be lower than other sectors such as banking or gambling as insurance products offer limited flexibility to criminals. Indeed, in the *National Money Laundering and Terrorist Financing Risk Assessment of Mauritius* (NRA) (August 2019), the Insurance Sector was identified as having medium ratings for Money Laundering Sectorial Vulnerability and Money Laundering Sectorial Risk, and a medium-low rating for Money Laundering Sectorial Threat. However, the risk of illicit funds being placed in the financial system via Insurance products remains as criminals will always endeavour to target sectors where the overall risk of detection is deemed lower. Hence, raising AML/CFT awareness in the Insurance Sector remains an ongoing process at the level of the FIU.

MISUSE OF INSURANCE SECTOR

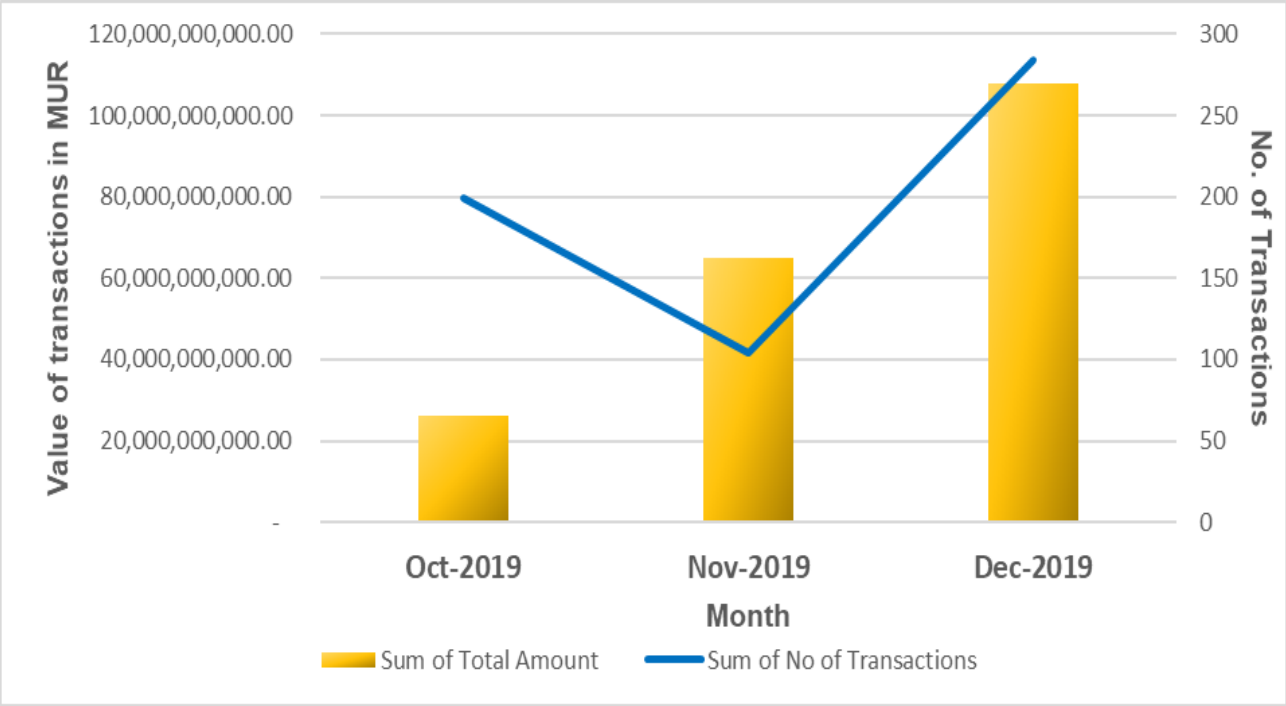
Red Flags:

- ⇒ Client wants to use cash for a large transaction;
- ⇒ Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account;
- ⇒ Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;
- ⇒ Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
- ⇒ Client conducts a transaction that results in a conspicuous increase in investment contributions;
- ⇒ Scale of investment in insurance products is inconsistent with the client's economic profile;
- ⇒ Unanticipated and inconsistent modification of client's contractual conditions,
- ⇒ Including significant or regular premium top-ups;
- ⇒ Unforeseen deposit of funds or abrupt withdrawal of funds;
- ⇒ Involvement of one or more third parties in paying the premiums or in any other matters involving the policy;
- ⇒ Overpayment of a policy premium with a subsequent request to refund the surplus to a third party;
- ⇒ Funds used to pay policy premiums or deposits originate from different sources;
- ⇒ Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions;
- ⇒ Client cancels investment or insurance soon after purchase;
- ⇒ Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner;
- ⇒ Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract;

Source: http://www.fiumauritius.org/English/Guidelines/Pages/default.aspx (Suspicious Transaction Report – Guidance Note 3 (2014))

Value of transactions reported

For the 178 STRs reported via goAML application/ paper submission during the period under review, more than 580 transactions with an aggregate value of approximately MUR 199 billion[1] were reported, with roughly 54% of this aggregate value reported during the month of December 2019 alone.



[1] Transactions reported through goAML have been effected in various currencies such as the USD and the EUR. Figures in this publication are expressed in MUR for ease of analysis. Caution should be exercised in interpreting these figures as they only represent transactions deemed as suspicious by reporting persons while making the reports. It also includes proposed and attempted transactions, which may involve inflated values due to attempts by perpetrators to abuse the financial system.

Compared to the last quarter, the aggregate value reported during this current quarter has reached epic proportions, with a staggering increase of more than 3300%, with more or less 8000% increase in the Banking sector and the Insurance sector alone!

A closer scrutiny of the STRs show that more than 90% of the aggregate value reported were proposed/ attempted high-value transactions that were suspected to be scams through the use of fake letter of credits, bank guarantees, swift messages or emails. These suspicious transactions did not materialise as the reporting persons in the financial sector are well versed in detecting such alleged scams. Reporting persons should however remain vigilant as these banking instruments continue to be targeted by criminals. With some cause of alarm, it has been observed that in some of the suspected scams reported the potential victims (or possibly intentional / unintentional accessories) were identified as either well established local businesses or local gatekeepers of the financial system. This indicates that despite the lack of sophistication in such scams – with unbelievable huge figures – anyone can still fall prey to these confidence tricks.

TYPES OF FRAUD

Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination. Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

Other letter of credit frauds occur when con artists offer a "letter of credit" or "bank guarantee" as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment "opportunities" simply do not exist.

Tips for Avoiding Letter of Credit Fraud:

⇒ If an "opportunity" appears too good to be true, it probably is.

⇒ Do not invest in anything unless you understand the deal. Con artists rely on complex transactions and faulty logic to "explain" fraudulent investment schemes.

⇒ Do not invest or attempt to "purchase" a "letter of credit." Such investments simply do not exist.

⇒ Be wary of any investment that offers the promise of extremely high yields.

⇒ Independently verify the terms of any investment that you intend to make, including the parties involved and the nature of the investment.

Source: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/letter-of-credit-fraud

Prime Bank Note Fraud

International fraud artists have invented an investment scheme that supposedly offers extremely high yields in a relatively short period of time. In this scheme, they claim to have access to "bank guarantees" that they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of "bank guarantees" can be sold at a two percent profit on 10 separate occasions—or "traunches"— the seller would receive a 20 percent profit.

To make their schemes more enticing, con artists often refer to the "guarantees" as being issued by the world's "prime banks," hence the term "prime bank guarantees." Other official-sounding terms are also used, such as "prime bank notes" and "prime bank debentures." Legal documents associated with such schemes often require the victim to enter into non-disclosure and non-circumvention agreements, offer returns on investment in "a year and a day," and claim to use forms required by official authorities.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank, where it is eventually transferred to an off-shore account in the control of the con artist. From there, the victim's money is used for the perpetrator's personal expenses or is laundered in an effort to make it disappear.

While foreign banks use instruments called "bank guarantees" in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

Tips for Avoiding Prime Bank Note Fraud:

⇒ Think before you invest in anything. Be wary of an investment in any scheme that offers unusually high yields by buying and selling anything issued by "prime banks."

⇒ As with any investment, perform due diligence. Independently verify the identity of the people involved, the veracity of the deal, and the existence of the security in which you plan to invest.

⇒ Be wary of business deals that require non-disclosure or non-circumvention agreements that are designed to prevent you from independently verifying information about the investment.

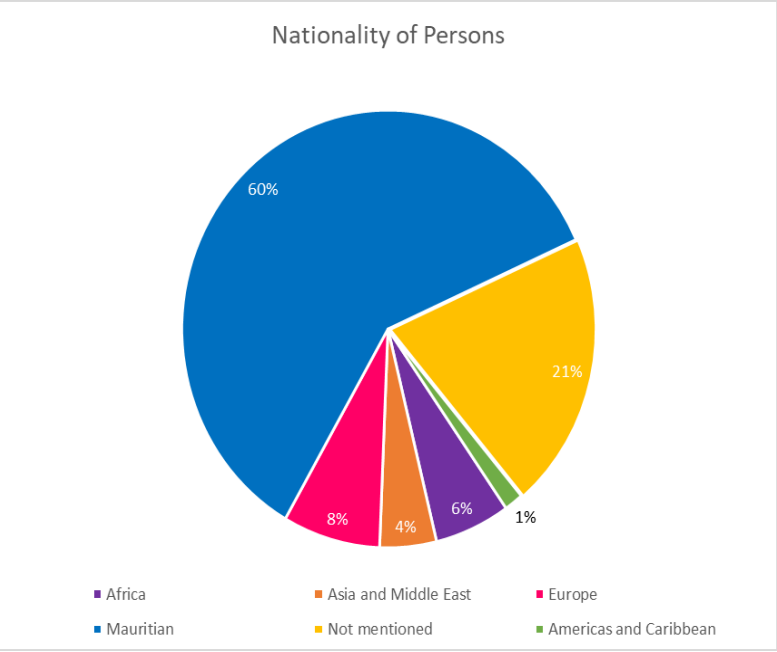
Source: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/prime-bank-note-fraud

Composition of STRs

Elements in any STR can be categorised as **Person** (i.e. natural persons), **Entity** (i.e. legal persons/ arrangements) or **Account** (i.e. accounts held by Persons/ Entities at Banks or Financial Institutions). Thus, observations of trends in the types of Persons, Entities and Accounts involved can be derived from the aggregate of STRs filed in the quarter ended 31 December 2019. Two critical points should however be stressed upon. First, information contained in STRs must be treated with care as they contain unsubstantiated allegations of *possible* criminal or suspicious activities, akin to confidential informant tips. As such, while any observed trend may provide useful and potential parameters for monitoring, STR information cannot be readily interpreted as conclusive evidence of any criminal or improper conduct. Second, when STRs are filed at the FIU, the types of Persons, Entities and Accounts can be connected to reports in a number of ways e.g. alleged perpetrators, alleged victims, persons/ entities directly or indirectly involved in the suspicions being reported etc. Consequently, it is not necessary that any observed trend is indicative of an increase in risk in a particular type of Person, Entity or Account.

Type of Persons

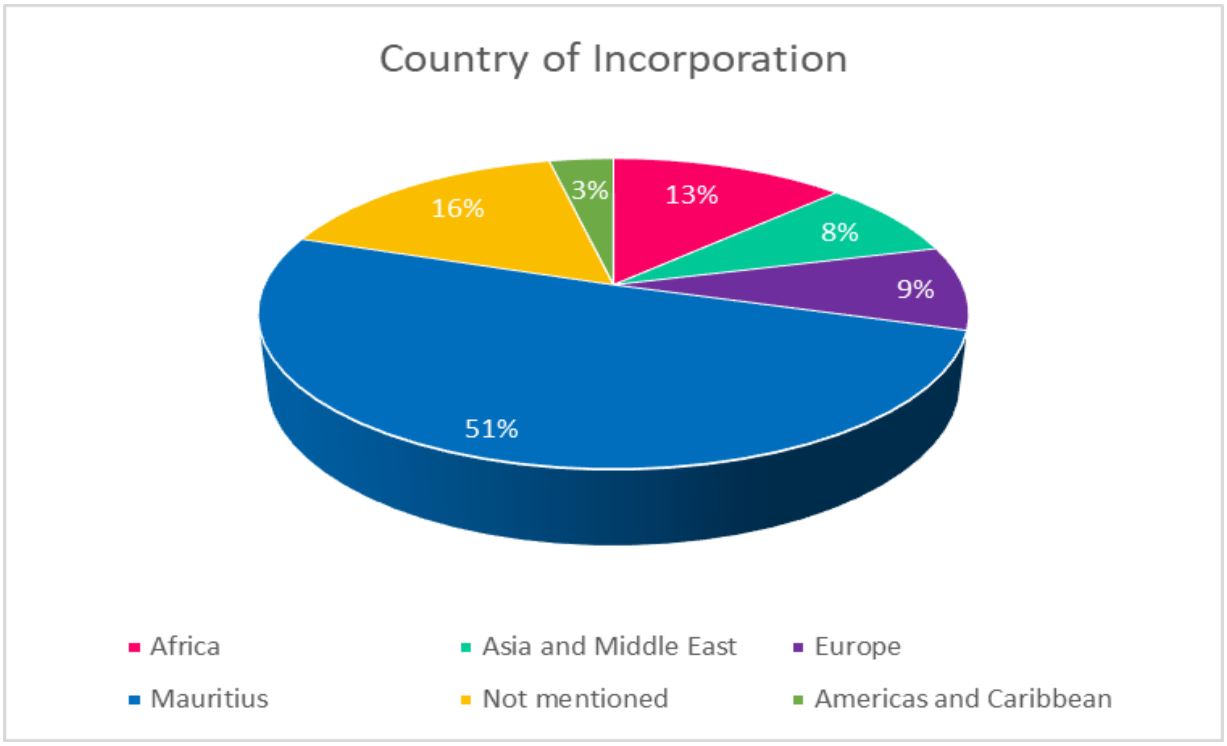
As shown in the following chart, 60% of persons involved in STRs are Mauritian nationals. Also, a substantial 21% could not be identified by the reporting persons. This could be explained by the fact that some reported suspicious transactions are proposed or attempted transactions that have not materialised and for which no identification details could be obtained by reporting persons.

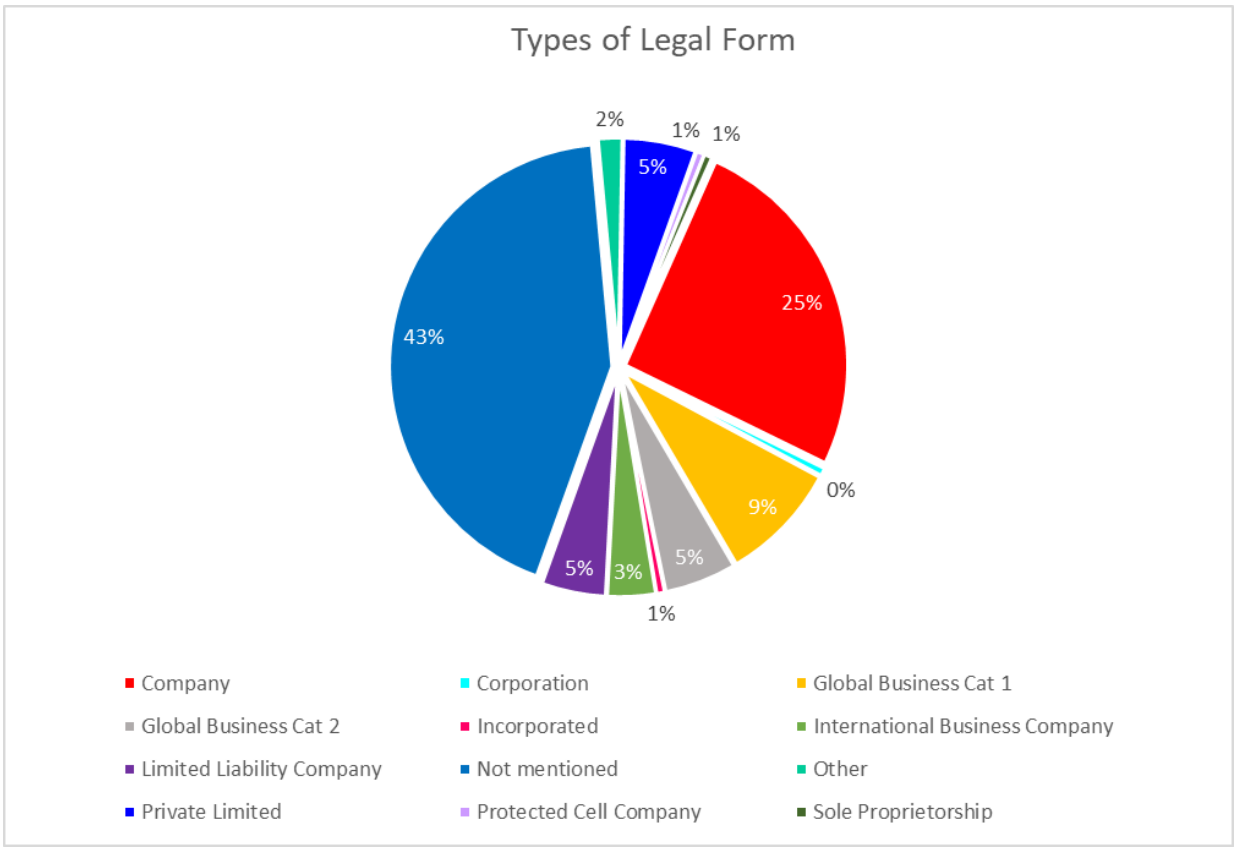


However, as already highlighted earlier on pages 3 and 4, some reporting persons, based on the specificities of their industry, face difficulties in securing 'Know Your Client' information or transaction information. Reporting persons are hereby reminded that the FIAMLA and its regulations require them to obtain and keep records of identity of customers as well as records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction.

Type of Entities

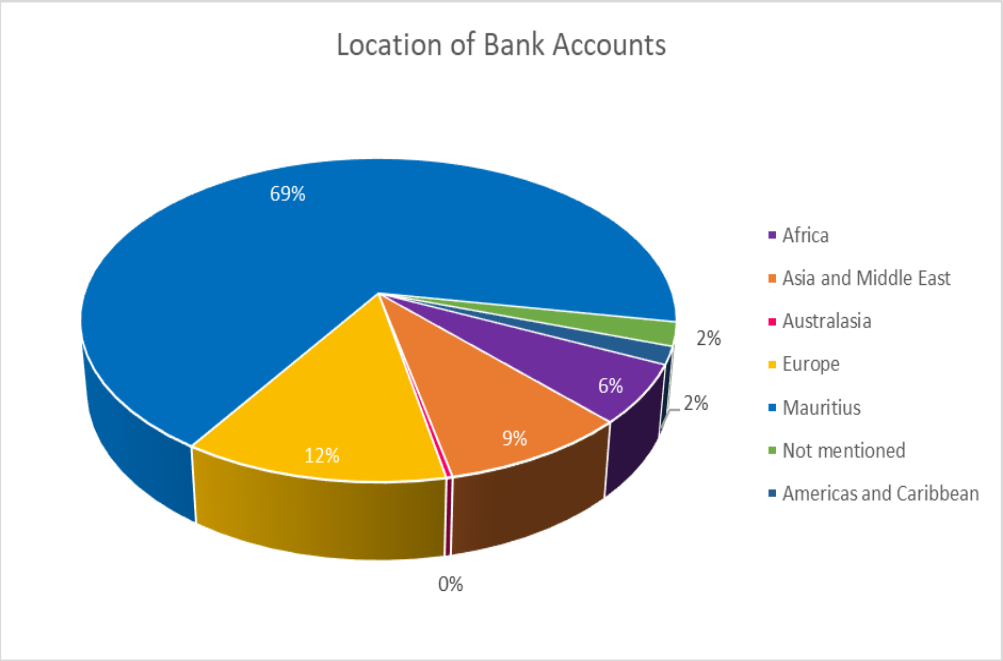
During the quarter ended 31 December 2019, 51% of entities involved in STRs were incorporated in Mauritius while 13% were incorporated in the African region. Here also, it is observed that for 16% of entities in the reports, reporting persons could not trace their jurisdictions.





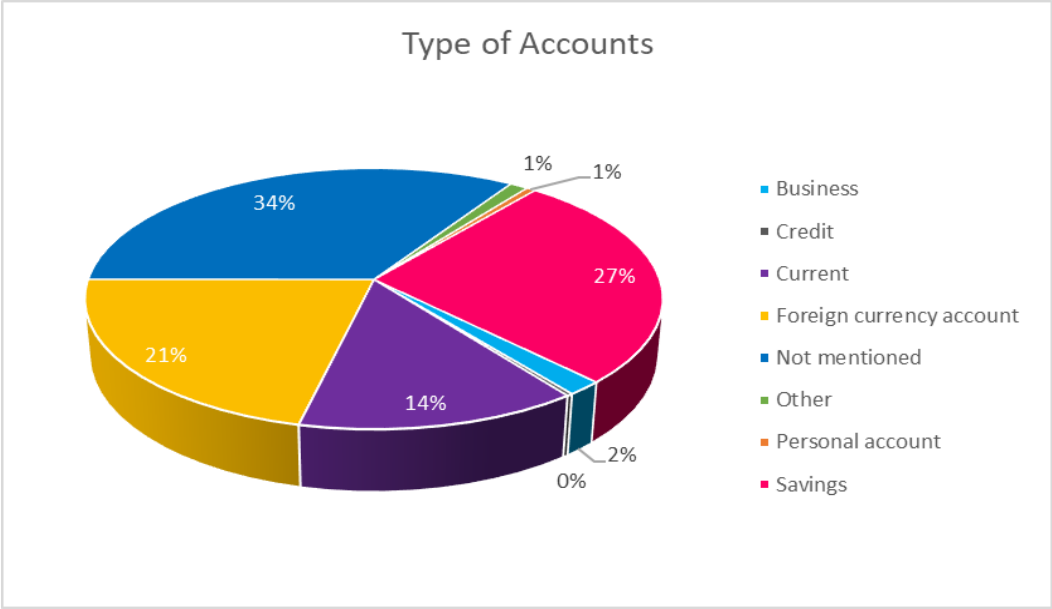
Type of Accounts

For the quarter ended 31 December 2019, more than 300 bank accounts were traced in STRs, with about 50% held by individuals, 30% held by entities and 20% the ownership of which was not identified. Unsurprisingly, as most transactions reported are bi-party transactions[2], 69% of the bank accounts are Mauritian bank accounts. The foreign counterparties to transactions appear to hold their bank accounts mostly in the European, Asian/ Middle Eastern and African region.



[2] *A **Bi-Party** transaction is a transaction with a clear "from" and "to" sides, i.e. the transaction initiated **from** a Person/ Entity/ Account, in favour of (**to**) another Person/ Entity/ Account*

In terms of banking products, where identifiable, Savings accounts, Foreign currency accounts and Current accounts have been most used in the aggregate STRs received during the current quarter.



DID YOU KNOW?

According to the *General Glossary* of the Financial Action Task Force (FATF) Recommendations, a Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. This definition is also reflected in the FIAMLA and the Companies Act 2001.

Identifying beneficial ownership is one of the central themes of the FATF Recommendations, especially under Rec 24 where countries should take measures to prevent the misuse of legal persons for ML/TF by ensuring that there is *adequate*, *accurate* and *timely* information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. Countries are also encouraged to take measure measures to facilitate access to beneficial ownership and control information by financial institutions and designated non-financial businesses and professions undertaking the requirements as set out in Recs 10 and 22 (i.e. Customer Due Diligence). Compliance with Rec 24 is intrinsically linked with the effectiveness of the measures assessed in Immediate Outcome 5 to prevent the misuse of legal persons for ML/TF.

In October 2019, the FATF issued its *Best Practices on Beneficial Ownership For Legal Persons*. In this publication, the FATF has finalised best practices with examples from across the global network of FATF and FATF-Style regional bodies' members, which will help countries implement the FATF's requirements. The report highlights that jurisdictions using a 'multi-pronged approach' with several sources of information are often more effective in preventing the misuse of legal persons for criminal purposes. The 'multi-pronged approach' recommends that countries should use one or more of mechanisms (the *Registry Approach*, the *Company Approach* and the *Existing Information Approach*) to ensure that information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or can be otherwise determined in a timely manner by a competent authority. For an effective implementation of the 'multi-pronged approach', the report also highlights the suggested roles and responsibilities of different key stakeholder in the AML/CFT framework. For instance:

Companies and legal persons

- ⇒ Provide basic and beneficial ownership information for the company registry upon registration, annually and when changes occur without delay to ensure that the information is up-to-date.
- ⇒ Obtain updated information from their shareholders.
- ⇒ Seek to apply restrictions against shareholders for failure to provide beneficial ownership information through appropriate courts or authorities, such as in relation to shareholder voting rights, or the sale of shares.
- ⇒ Understand and/or hold information on their ownership structure, including chain of ownership.

Shareholders

- ⇒ Provide accurate information on beneficial ownership and updates on changes to beneficial ownership without delay.

Reporting persons

- ⇒ Understand the ownership and control structure of the customer, and understand the ML/TF risks in relation to legal persons.
- ⇒ Adequately carry out CDD measures at the incorporation stage and conduct ongoing CDD on the business relationship to make sure that the information on beneficial ownership is accurate and up-to-date, and scrutinise transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and its business and risk profiles, including, where necessary, the customer's source of funds.
- ⇒ Record the CDD procedures performed and maintain these records for at least five years.
- ⇒ Report suspicious transaction activities.

Source: http://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf

Indicators in STRs

Registered users on goAML who file STRs are required to classify the STR being submitted in terms of any applicable "suspected predicate offence" and "suspected typology" (i.e. indicators) that may have been derived from the grounds for suspicion of the STR. Any "suspected predicate offence" and "suspected typology" that reporting persons may associate to the reports being filed represent only suspicions and perceptions of threat identified at the time of detection of the suspicious transactions being reported and based on information available at level of MLROs. Hence, while indicators may provide useful information on the perceived ML/TF threat trends, they should not be interpreted as being conclusive evidence of any criminal offence that may have occurred.

For any STR filed, there can be one or more suspected predicate offence or typology. Currently, the FIU has not imposed a strict requirement for registered users on goAML to add indicators to their STRs. As such, some of STRs filed during the period under review do not contain any indicators.

Data analysed on goAML shows that the main indicators for "suspected predicate offence" include *Money Laundering*, *Fraud* and *Tax evasion / Smuggling / Tax Crimes*. Although the indicator Money Laundering offence continue to be selected in most STRs, reporting persons appear to be identifying better other indicators as shown in the increased figures. **In order to generate more meaningful statistics on indicators trends, reporting persons are hereby encouraged to also add an indicator for the perceived alleged predicate offence whenever they select 'Money Laundering offence' from the list of indicators.**

Indicator	Oct-2019	Nov-2019	Dec-2019	Grand Total
Money laundering	24	9	42	**75**
Fraud	14	5	9	**28**
Other	8	4	10	**22**
Tax evasion / Smuggling / Tax Crimes	2	6	8	**16**
Forgery	4	1	1	**6**
Corruption	-	-	2	**2**
Participation in organised criminal group / racketeering	-	-	1	**1**
Terrorism/terrorist financing	-	-	1	**1**
Robbery or theft	1	-	-	**1**
Illicit arms trafficking	-	-	1	**1**
Grand Total	**53**	**25**	**75**	**153**

Additionally, the main indicators for "suspected typology" include *Activities that do not match the client profiles* and *Suspicious behaviour/ reluctance to provide details*.

Indicator	Oct-2019	Nov-2019	Dec-2019	Grand Total
Activity does not match client profile	17	13	35	**65**
Suspicious behaviours / Reluctance to provide details and documents	21	12	30	**63**
Use of casinos and gaming activities	-	-	10	**10**
Use of offshore financial services	3	1	1	**5**
Structuring	1	-	3	**4**
Smurfing	-	1	3	**4**
Use of family members and third parties	1	1	1	**3**
Use of nominees and trusts	1	1	-	**2**
Trade based money laundering	1	-	-	**1**
Grand Total	**45**	**29**	**83**	**157**

WHO SHOULD REPORT STR?

Section 14(1) of FIAMLA states that the following persons shall, as soon as practicable but not later than 15 working days from the day on which they become aware of a transaction which they have reason to believe may be a suspicious transaction, make a report to the FIU of such transaction:

- ⇒ Bank,
- ⇒ Financial institution,
- ⇒ Cash dealer,
- ⇒ Controller or auditor, other than the Principal Co-operative Auditor of a credit union under the Co-operatives Act
- ⇒ Member of a relevant profession or occupation.

Currently, not all of the above reporting persons are registered on goAML. Although the FIU has progressively opened goAML registration to some reporting persons (namely, banks, financial institutions, cash dealers and auditors), not all of these reporting persons have elected to register on goAML. Hence, in order to increase registration on goAML and the number of online filings of STRs, the FIU has already embarked on an outreach program, in collaboration with relevant supervisory authorities, to encourage registration on goAML and provide training on the use of goAML (including refresher trainings to new users of organisations already registered). Moreover, on 09 November 2019, the Regulations under Sections 14C and 35 of FIAMLA were enacted requiring:

> *3. (1) For the purpose of section 14C of the Act, every reporting person shall, through its Money Laundering Reporting Officer, make an application electronically for registration.*
>
> *(2) Where, pursuant to regulation 26(3) of the Financial Intelligence and Anti-Money Laundering Regulations 2018, a reporting person is unable to appoint a Money Laundering Reporting Officer, the reporting person shall make the application for registration with FIU.*
>
> *(3) An application for registration under paragraph (1) or (2) shall, in relation to such category of reporting persons as FIU may determine, be made note later than such period as FIU may determine.*

In the above context, the FIU shall issue guidelines that will include the category of reporting persons referred to in regulation 3(3) and the period within which each category shall make an application for registration.

Contact Us

Financial Intelligence Unit

10th Floor, SICOM Tower

Wall Street

Ebene Cybercity

Ebene

72201

Telephone: (230) 4541423

FAX: (230)4662431

Email:fiu@fiumauritius.org

goAML Helpdesk
Email: goamlhelpdesk@fiumauritius.org