
Financial crime insights: **Money laundering risks associated with money mules**

June 2024



What is a money mule?

Money mules are individuals who are recruited to help launder the proceeds of crime or physically transport goods, merchandise, or money on behalf of a criminal.

Persons being used as money mules may be knowingly or unknowingly complicit in the laundering of funds, thereby helping criminals to profit from illicit activities.

Criminals use money mules to conceal the origin of their illicit funds and ultimately benefit from the proceeds of crime. By using the accounts of money mules to receive and transfer these proceeds, the mules help to create distance between the criminal and their ill-gotten gains.

Executive summary

The use of money mule accounts is commonly used in financial schemes, illicit financial flows, romance scams, job scams and a myriad other scams. These are serious crimes which generate proceeds from unsuspecting victims, who unwittingly send money to the bank accounts of money mules, for use by the criminals who take over the money mules' accounts. Criminals use money mules to obfuscate the flow of money which benefits them.

Money muling is often a precursor to or part of other criminal activities such as identity theft and money laundering which adds to its complexity and complicates the detection and prevention of this crime.

In developing this publication, the Financial Intelligence Centre (FIC) reviewed suspicious and unusual transaction reports (STRs) regarding money mules submitted by accountable institutions, during the period August 2016 to July 2023.

The FIC set out to include a search of the database of keywords used by accountable institutions associated with money mule activities. The keyword search proved insufficient, however, as accountable institutions do not explicitly refer to money muling when filing regulatory reports with the FIC. Account behaviour proved to be more useful indicators of money mule activity.

During the review of the suspicious and unusual transaction report database, the FIC identified 58 cases referring to money muling and related illicit flow of funds for its analysis. The contents of 153 section 29 regulatory reports linked to the 58 cases were analysed to extrapolate trends, role players,

occupations, and business entities involved in money mule activity.

The FIC's analysis found extensive use of shell companies to host fraudulent funds, while South Africans were identified as directors or signatories of entities implicated in money muling or illicit financial flow activities. The majority of money mule activity identified in the review took place in the Gauteng and Western Cape provinces.

In some instances, South Africans received funds via money remitter transactions from foreign jurisdictions with no clear purpose for the funds and unknown relations between the sender and the receiver.

There was a prevalence of crypto assets being used in money mule activity, with suspected accounts reflecting high-value daily cash deposits in the banks, followed by rapid transfers to crypto asset service providers.

There was also pervasive use of shell companies to receive fraudulent South African Revenue Service (SARS) refunds in high-value amounts.

Some accountable institutions filed defensive suspicious and unusual transaction reports in response to adverse media, subpoenas or section 27 requests for information from the FIC.

The learnings gleaned from the case analysis are reflected in this report which should be useful to accountable institutions. As a result of this report, the FIC has embarked on expanding the list of indicators relating to money mules on its registration and reporting system, goAML, to enhance categorisation of money muling and related financial crimes.

Introduction

In 2023, the FIC conducted a preliminary risk assessment of the inherent money laundering and terrorist financing (ML and TF) risks related to money mules. The risk assessment offered initial observations on this crime type.

In this *Financial Crime Insights* report the FIC aims to assist government, financial and non-financial institutions and other stakeholders better understand and identify money mule activities and schemes and help with developing effective strategies to address this crime type.

This report focuses on threat patterns and trend information identified through analysis of suspicious and unusual transaction reports (STRs) and suspicious activity reports (SARs) submitted to the FIC between August 2016 to July 2023.

The FIC reviewed the data contained in the STRs and SARs to enrich understanding of the characteristics of money mule actors, their sources of funds, financial flows, and payment methods

related to this type of crime. The aim was to build profiles that could be used by accountable institutions to fine tune transaction monitoring rules to improve detection of money mule related transactions, improve intelligence gathering, and perform targeted analysis on identified and related transactions.

The report includes a compilation of money laundering indicators flowing from the analysis of FIC transaction reports related to money mules and supported by analysis of domestic and international sources.

These observations are intended to assist in identifying instances of suspicious and unusual transaction activity related to money muling. The indicators are intended to assist in adopting preventive measures including implementing a risk-based approach and a stimulus for business to submit detailed STRs and other regulatory reports to the FIC.

Background

The Financial Action Task Force (FATF)¹ defines a money mule as a person or people who are used to transfer value, either by laundering stolen money or physically transporting goods or other merchandise.

Money laundering occurs when criminals conceal, disguise, and transform money obtained from unlawful activity to make it appear legitimate. In money muling, criminals use the account holder to function as a money mule to facilitate money laundering.

Money muling has been around for a long time and is a growing transnational crime. It is well organised, and often integrated into various predicate crime types as a precursor to money laundering. Money muling is often the approach used by criminals when they want to target or perpetrate specific crimes. While money mules may not be directly involved in these crimes, through the use of their accounts and/or identities they facilitate criminals laundering and profiting with impunity from crimes ranging from human trafficking, drug smuggling, moving money across borders illegally, fraud, and cybercrime.

In a sense, money mules can be seen to be witting or unwitting accomplices to criminal activities.

Literature shows that often criminals will recruit money mules to illicitly move money out of South Africa.

Criminal sub-groups may also be loosely organised and de-centralised across different jurisdictions, which further complicate efforts to investigate money muling activity.

It is not unusual for money mules to be recruited to open accounts on a variety of financial sector platforms such as banks, crypto asset service providers or money remitters. Money muling is also attractive to syndicates involved in human trafficking or kidnappings, illicit flow of funds across borders, money laundering, fraud and other crimes. Criminals who recruit money mules to act on their behalf knowingly do so that their own association to the crime perpetrated is diminished allowing them to avoid detection and liability.

Often groups and professional enablers are involved in money muling. Networks of money mules can also include shell companies and legitimate businesses.

¹ <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf>

These networks also feature different types of financial institutions, including banks, payment and remittance providers, and crypto asset service providers (CASPs)².

To further conceal the financial trail of their ill-gotten gains, criminals involved in money muling use a variety of channels to launder their proceeds in the financial system such as banking services, trade-based money laundering (TBML), money remittances and unlicensed services such as hawala. Technology has enabled money mules to develop and increase the scale, scope, and speed of their illicit activities. Furthermore, technology offers platforms and tools criminals abuse for extracting as much money as possible from their victims. Money mule syndicates are exploiting development in financial technology to make it easier and faster to launder their proceeds.

Digital financial services such as remote online account opening also allow criminals to easily set up

accounts and launder their illicit proceeds. In addition, these criminals are taking advantage of social media and messaging platforms to recruit money mules across borders.

Proceeds can be laundered quickly through a network of accounts which often span multiple jurisdictions and financial institutions.

This report lists risk indicators, profiling of possible money mules perpetrators, transaction locations, types of industries involved as well as useful account information and controls that may be useful for public and private sector entities to detect and prevent money muling, illicit financing, and related money laundering.

FATF notes that money mules may be knowingly complicit in the laundering of funds or work unwittingly, or negligently, on behalf of a professional money laundering network or organised crime group.

Some ways in which money mules are used:

- Unwitting - Individuals who are unaware they (and/or their bank accounts) are being used to facilitate criminal activity. Fraudsters often use these mules to move or accept money on their behalf.
- Wilfully blind - The mules may suspect the source of the money they are moving is not legitimate. These individuals may decide to use what they earn as money mules to make a living, supplement their regular income due to financial difficulties or greed.
- Complicit - These individuals are aware they are involved in criminal activity and engage in it wilfully. This can range from innocent or naïve individuals who are unaware of what they are doing, to more experienced, adept fraudsters involved in money muling rings.
- Take over of identity or identity fraud - The recipient account is created by fraudsters who have taken over the victim's identity to receive fraudulent money

Criminals who commit cybercrime, conduct fraudulent schemes, and orchestrate the illegal flow of money, recruit people as money mules to facilitate transactions on their behalf. These criminals use money mules to avoid liability, obfuscating the flow of illicit money to profit from their crimes.

Criminals may offer payments or some sort of gratuity to money mules who hand over control of their bank accounts to facilitate unlawful activities.

The COVID-19 pandemic saw a significant increase in money muling. According to FSCA (Financial Sector Conduct Authority) criminals were

opportunistic in committing crime during the pandemic. During this time, criminals turned to unregulated financial services, scamming desperate job seekers, who were potentially vulnerable to being exploited as money mules.

Money mules can be of any age, race, or gender and may be willing or unknowing participants or can be actively recruited. They are recruited via false recruitment advertisements for 'transaction managers', through face-to-face engagement by criminals, online via social media interactions and through other means. Money mule recruiters are also known as mule 'herders.'

²<https://www.fscsa.co.za/News%20Documents/FSCA%20Press%20Release%202020%20FSCA%20cautions%20consumers%20against%20mule%20bank%20account%20scams.pdf>

How criminal organisations recruit money mules:

- Job scams - Individuals are contacted about a new job without having applied for the position and where the “employer” does not provide any details about their company
- Investment scam - An individual(s) receives a text message or e-mail notification urging them to make an investment, usually urgently, with a promise of a big return
- Romance scam - Usually online contact via social media or online dating platforms
- Impersonation scam - Calls, messages and e-mails conducted by individuals claiming to be from big organisations or government agencies asking for personal details or bank details.

Purpose of this report

The FIC conducted a review and analysis on money laundering and terrorist financing risks associated with money mules. This report assesses the threats associated with professional money launderers (PMLs) and vulnerabilities associated with money mules. **The report aims to:**



Raise awareness on the unique characteristics of PMLs



Improve understanding of the **role and functions** of those involved in money mules



Understand the **business models and specific functions** performed by PMLs



Understand how **organised crime groups use the services** of PMLs to move funds



Identify relevant **money laundering typologies and schemes**



Develop **risk indicators on PMLs for law enforcement**, other competent authorities and the private sector



Provide **recommendations for the detection**, investigation, and prevention of PML

Data mining from suspicious and unusual transaction and activity reports

The FIC analysed regulatory reports filed by accountable institutions that noted suspected money mule activities. The methodology used to extract and analyse the data included:

- Section 29 reports (suspicious transaction reports and suspicious activity reports) linked to cases relating to money mules and illicit flow of funds
- 58 cases relating to money mules and illicit flow of funds were identified and extracted against the FIC STR and SAR database for the period May 2019 to November 2023. However, some of the section 29 reports were linked to cases cited from August 2016 to July 2023.
- 153 section 29 regulatory reports linked to the 58 cases were analysed and categorised according to the various crime types:
 - Money mules-related reports
 - Illicit flow of funds - specifically reports relating to crypto asset schemes
 - Potential or suspected money mules related reports
 - Kidnapping
 - Fraud and scams.

Only the categories above were considered during analysis in mapping common trends or role players involved in money muling. No direct linkages to money mule crimes were found in the regulatory reports under the 'potentially money mules related' category on the FIC's registration and report system, goAML. This was as reporters did not specify money mule related crimes. The profiles and transacting behaviours of individuals in the five categories are often similar to what is found in the

'money mule related reports'. But, without further corroborating information, the link could not be established and no further assumptions could be made.

The contents of the regulatory reports in the 'possible money mule' category was considered to identify common trends, role players and individual profiling on facts contained in the regulatory reports.

Analysis of the reports

Section 29 regulatory reports received from accountable institutions were extracted from the FIC database to mine them for their data on money mules, to help identify the role players, the flow of funds, any complex structures, jurisdictions, the types of accounts used, and any other related information.

Data mining involved a process of extracting and analysing large amounts of data from the FIC's suspicious and unusual transaction report database to identify patterns and trends.

Findings - report level

Number of reports

Banks, CASPs and foreign exchange dealers submitted the highest number of section 29 regulatory reports in the period 2016 to 2023.

Other sectors such as high-value goods dealers, investment advisors or intermediaries and cross-border money or value transfer service providers are also considered high risk sectors for money muling.

The majority of the section 29 regulatory reports filed by the banking sector did not clearly state the activity that transpired between the bank and their clients. The information provided mostly related to the movement of funds in a client's account, usually reported as being inconsistent with the client profile or expected transactional behaviour. Several of the 153 STRs examined also identified the suspicion of possible romance scams, job scams and impersonation or third-party transactions.

Table 1: Number of reports relating to money mules

Schedule item	2016	2017	2018	2019	2020	2021	2022	2023	Grand total
Banks	2	13	10	19	17	26	40	10	137
High-value goods dealers* (motor vehicle dealers)						1	1		2
Crypto asset service providers* (general)							6	3	9
Investment advisors or intermediaries							1		1
Foreign exchange agent or companies			1		2				3
Cross-border money or value transfer services provider							1		1
Grand total	2	13	11	19	19	27	49	13	153

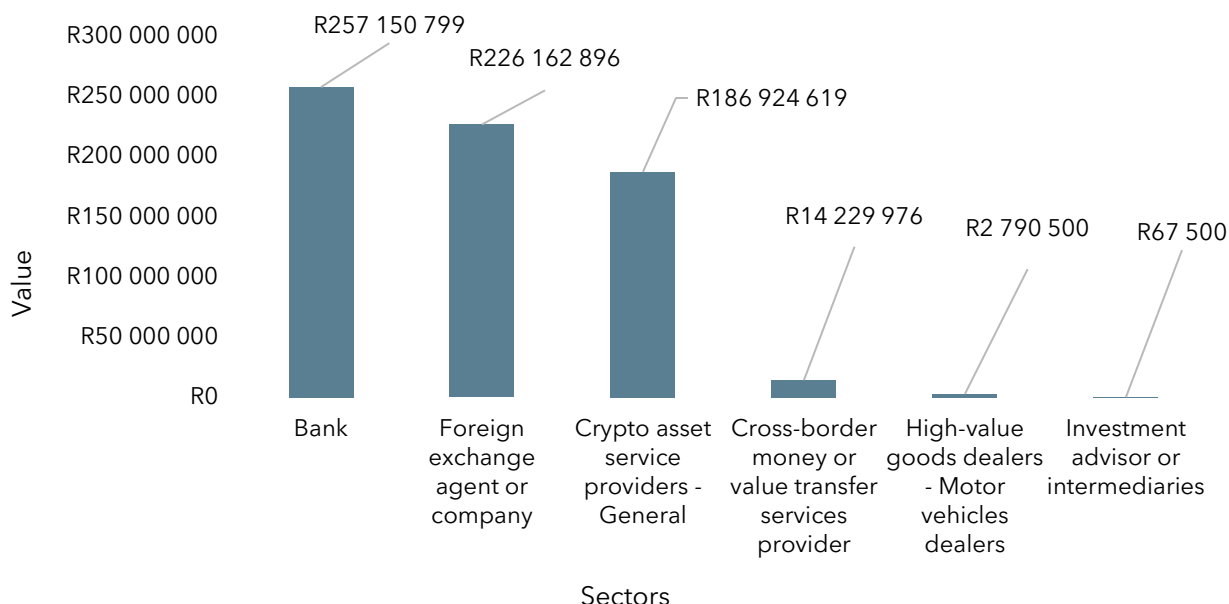
* High-value goods dealers and crypto asset service providers were included as Schedule 1 items in the Financial Intelligence Act at the end of 2022.

Value of regulatory reports

The banking sector recorded the highest rand value of all the reports relating to money mules in the 2021 and 2022 calendar years. During the report analysis period (2016 to 2023), the FIC noted fewer section 29 reports linked to money mules filed by

foreign exchange agents or companies, investment advisors or intermediaries and CASPs. This was likely due to insufficient information provided regarding the value of the transactions or because fewer section 29 regulatory reports were filed by these sectors.

Figure 1: Value of section 29 reports linked to the 58 cases from May 2019 to November 2023



Account behaviour

The highest number of regulatory reports for both the incoming and outgoing movement of funds were linked to current, transmission and business accounts. Several current accounts were reported for the suspicion of possible third-party transactions. These types of transactions involve an individual opening an account and handing over their bank card, account number and/or the login details to another person who anonymously transacts using that account.

Third-party transactions also include individuals opening accounts and performing transactions on

behalf of other individuals. This enables the movement of funds through layering between the accounts. The funds are then withdrawn in cash at different locations and from ATM machines countrywide.

Through the analysis the FIC found that individuals implicated in this type of crime are often unemployed, pensioners, and young South Africans such as students. A small percentage of foreign nationals' accounts were also identified for potential involvement in money mule activity during the data mining process.

Suspicious account indicators included:

- Business accounts not displaying business expenditure such as salaries and tax payments
- Personal accounts not displaying salary credits, living expenses and debit orders
- In many cases there appeared to be a rapid disposition of funds after receipt
- Inability to confirm source of funds or wealth.

Table 2: Account activity reflecting flow of funds

Account name	Source account	Destination account	Total
Unknown account*	272	-	272
Current account	39	50	89
Transmission account	37	43	80
Business account	24	39	63
Cheque	25	18	43
Retail forex account	5	-	5
Bizlaunch account**	1	2	3
Money market account	1	1	2
Grand total	404	153	558

* Reporter could not establish the account type ** Start-up business account

Observations

The regulatory reports did not contain sufficient information regarding the activity or the transaction between parties in relation to money mule suspicions. Accountable institutions did not provide complete and sufficient information on suspected money muling in the regulatory reports they submitted to the FIC.

Several regulatory reports highlighted that the accountable institutions only became aware of the activity after they had received a subpoena from law enforcement and a case had been opened or an investigation lodged.

A significant number of regulatory reports submitted to the FIC relating to suspected money mule activity had insufficient information regarding the details of the type of accounts. This often happens when a suspicious transaction emanates from a bank account different to the accountable institution that reported the suspicion. When the suspicious transaction was conducted through other banks, the accountable institutions reporting the transaction will have insufficient information regarding the type of account involved. The information - such as the account type as well as the account number - will only be available to the accountable institution that initiated the transaction.

Type of industries linked to money mules

Cash and carry businesses, followed by construction companies, were identified as being involved in money mule criminal activity using shell companies. It was also discovered that most of the companies linked to suspected money muling activities were shell companies, where some were previously shelf companies. These companies were used specifically to conceal funds. The majority of these entities did not have any banking records, which is considered a normal business activity. Large amounts of funds entered these business accounts and were swiftly disposed of through various ways such as electronic funds transfers (EFT) and cash withdrawals.

The FIC found that the majority of these companies received fraudulent SARS refunds in high-value amounts. As part of its analysis, the FIC used different databases to supplement and verify the information contained in the regulatory reports. The majority of the companies involved in money mule activity linked to the fraudulent refund tax scams were based in Gauteng and had similar or shared directorships and signatories.

The FIC also found that some of these companies were undergoing liquidation or final deregistration






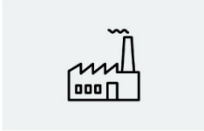










processes due to non-submission of annual returns to SARS.

While the companies used for fraudulent tax refund claims were registered between 2003 and 2022, it is believed the majority are shell companies given the lack of business activities noted in their accounts. These companies only received funds from SARS which was highlighted as refunds.

Most of these companies shared one or two similar directors which indicates potential collusion to facilitate criminal activities.

Where these company accounts received other income, the incoming payments usually emanated from other companies connected to the scheme. The payments received have no business purpose other than to increase turnover to create the impression that the companies are trading and generating income and are spending to sustain business operations. The directors or signatories of these companies were identified as young and older South Africans. A few foreign nationals were also identified, however, their involvement was a fraction compared to that of South Africans.

The following industries were noted in regulatory reports relating to money mule activities:

				
Construction	Cash and carry	Stockists of pipes, flanges, pipe fittings, bolting and general engineering for the oil, mining, and petrochemical industries	Consultants	Catering
				
Manufacturers	Transportation	Civil works	Engineering	Tent hire, chairs, and other related activities
				
Second-hand goods retailers	Hardware	Importers and exporters	Motor vehicle dealership	Warehousing
				
Steelworks				

Sectors identified in the regulatory reports

The top five banks in South Africa - FNB, Standard Bank, ABSA, Capitec and Nedbank - submitted the highest number and associated rand value of regulatory reports linked to money muling. Foreign exchange agents or companies, CASPs, cross-border money or value transfer services, high-value goods dealers (motor vehicle dealers) and investment advisors and intermediaries were also identified in the regulatory reports.

The majority of funds were moved electronically within South Africa with local electronic fund transfers making up the highest number of transaction modes as recorded in the reports. Some

of these transactions were a result of fraudulent SARS refunds made to shell companies.

Foreign exchange dealers or companies had a significant number of regulatory reports linked to money muling. The suspicious activity identified in this sector were linked to multiple entities involved in similar suspicious conduct.

CASPs reported suspected money mule activities due to the high volume of funds being transferred and potential exchange control contraventions. The transactions were primarily linked to romance scams, job scams, kidnappings, and investment scams related crimes.

Table 3: Sectors that filed regulatory reports on money mule activity

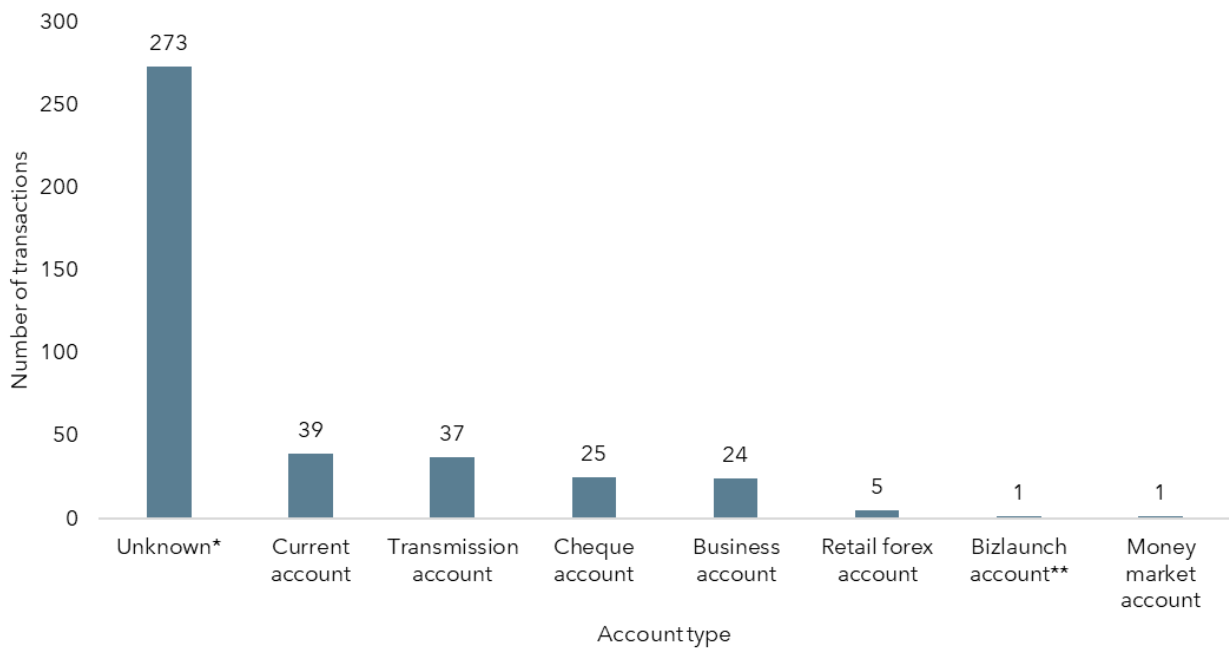
Schedule item	Source funds code	Total
Banks	Cash	124
	Electronic fund transfer (local)	637
	International funds transfer report (international inbound)	24
	International funds transfer report (international outbound)	44
	Money remittance	36
	Point of sale (POS)/card swipe	20
	Unknown	61
Foreign exchange agent or company	International funds transfer report (international outbound)	40
Crypto assets service providers (general)	Electronic fund transfer (local)	3
	Crypto currency	6
Cross-border money or value transfer services provider	Electronic fund transfer (local)	5
	International funds transfer report (international outbound)	1
High-value goods dealers (motor vehicles dealers)	Electronic fund transfer (local)	2
Investment advisor or intermediaries	Electronic fund transfer (local)	1
Grand total		1 004

Flow of funds related to money mule accounts**Incoming funds**

A variety of payment methods were noted in reports filed by accountable institutions for incoming transactions to accounts under investigation. The most common ways in which accounts received money was through unknown sources, current, transmission, cheque, and business accounts.

The majority of the unknown sources were mainly in the form of cash deposits where the details regarding the sources of funds could not be ascertained by the accountable institution due to insufficient information provided by depositors. The deposits were generally in rounded amounts, large amounts, with transactions conducted from various locations in South Africa, and multiple cash deposits.

Figure 2: Incoming funds - Source accounts



* Unknown - Reporter could not establish the account type

** Start-up business account

Outgoing funds

Outgoing funds from suspect accounts took place mostly through current accounts in different regions in South Africa, transmission, business, and cheque accounts. This included excessive card purchases

abroad, electronic transfers (including payments abroad), casino spend, airtime purchases, and money remitter transactions (payments described as gifts).

Other indicators relating to outgoing funds:








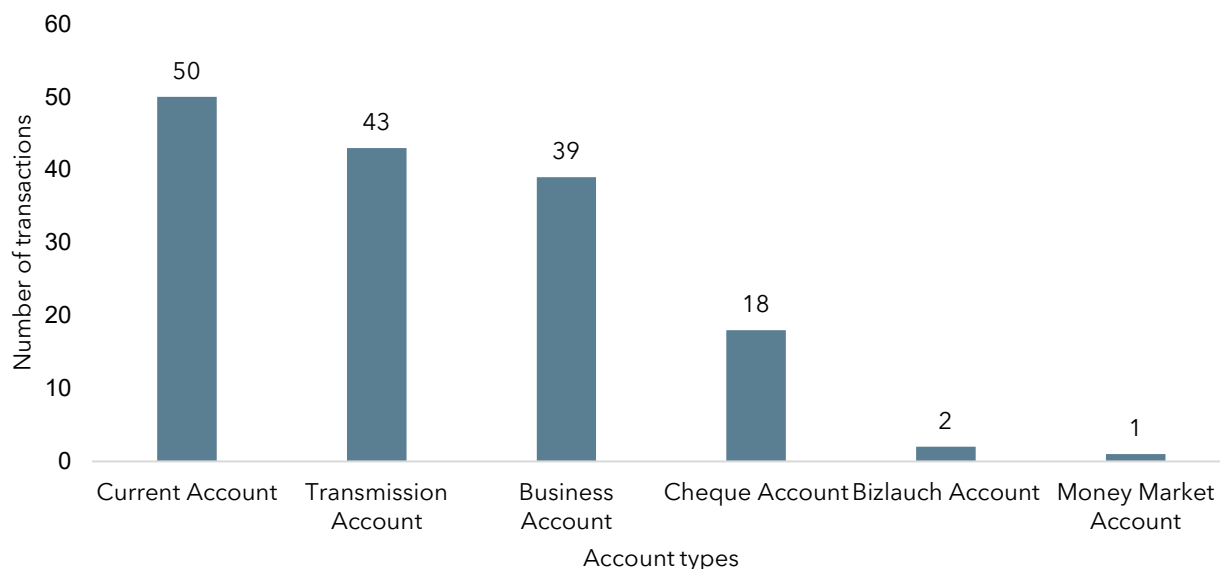
-  Disbursement of funds in short succession of receipt
-  Disbursement of funds in different geographical regions
-  High-value payments
-  Card purchases/point of sale purchases from the same place
-  Transfers to investment accounts
-  Immediate large cash withdrawals
-  Facilitation of gambling account

Figure 3: Outgoing funds - Destination account



* Standard Bank start-up business account

Modus operandi

Money muling

- Individuals send funds using a money remitter on behalf of a third party with the stated purpose of the funds being a gift. The accountable institution suspected that the individual who conducted the transaction could be a mule.
- Individual was accompanied by another into the premises of a foreign exchange agency to purchase foreign currency. The individual conducting the transaction brought large sums of cash to purchase foreign exchange currency. The accompanying person also conducted similar activities with other individuals or clients of the money remitter. The money remitter suspected the companion was using the money remitter's client to conduct transactions on their behalf.
- A bank reported a client for suspicious behaviour on their premises. The client was accompanied by another individual who gave instructions to bank personnel on the transactions.
- Account holders were reported for suspicious behaviour after remitting funds to the United Kingdom with no apparent reason and an unclear relationship between the sender and the receiver.
- A young individual received funds domestically from different senders based in South Africa. Over R300 000 was received in this individual's account and withdrawn in Lesotho. The accountable institution suspected that the young individual was being used as a money mule to facilitate the transfer of funds between the two countries.
- A female South African received funds from multiple senders based in the United States without a clear relationship between the sender and the receiver of funds. The accountable institution suspected that the client was being used as a money mule or involved in possible romance scams.
- An accountable institution flagged an individual for conducting rapid transactions. The individual used a betting account to facilitate these transactions and made multiple deposits ranging in value from R50 to R500, using vouchers from one of the third-party payment processors. The deposits were followed by EFT to a bank account and withdrawals without completing any wagering. All the funds deposited by the individual was done through a third-party payment processor and transferred via EFT. The individual was reported for possible mule activity.

- An individual in South Africa received funds from Ireland and sent the funds via a money remitter to multiple individuals in the Democratic Republic of Congo and France as gifts. The individual was reported for the suspicion of a third-party transaction or mule activity.
- A foreign national's account, which had been dormant for 10 months, was flagged over three suspicious transactions from South Africa to Nigeria. The accountable institution suspected money mule activity due to vague information between the sender and the receiver of the funds.

Structuring

- An individual received cash deposits into a credit card account which was opened in 1996 and closed in 2019. Suspicious activity noted in the account included numerous cash deposits which were disposed of through casino purchases. The accountable institution deemed the unknown source of funds coupled with numerous cash deposits as suspicious.
- An account received irregular, suspicious cash deposits from unknown sources. The funds were used immediately after receipt through transactions at casinos. Helping to evade detection, the cash deposits were made below the reporting threshold level.
- A public servant was reported for suspicious bank account activities. The account received funds from the state as well as numerous cash deposits, which were deemed suspicious and questionable by the reporting entity. The funds were disposed of through electronic payments between the employee's accounts which raised suspicions that the individual was camouflaging the true source of the funds. The reporting institution suspected that the individual was using his personal account for business-related activities.
- A business account was reported for suspicious activity due to the large, excessive funds received from large entities from a similar bank. The accountable institution suspected that the entity might be structuring the funds as the activity in the account did not match the business profile.

Fraud

- An entity was reported for tax fraud due to a large amount of funds credited in the entity's account from SARS. The funds were disposed of through an internet transfer to another entity's account referenced as maintenance. The entity was reported for suspicion of tax fraud.
- An individual was reported for being the secondary recipient of fraudulent SARS refunds. The funds were credited in the account of the entity and then transferred to the account of the subject. The accountable institution deemed the behaviour suspicious because of the individual's association with the entity which was implicated in the suspicion of fraud. Open-source information revealed that the subject was linked to another entity where she was co-director of an entity that received the fraudulent SARS refund. According to information provided by the accountable institution the subject worked in government.

Kidnapping

- Individuals were reported due to unusual, inconsistent movement of funds not in line with the profile of the account or expected transacting behaviour. The account was credited with salary payments, however, the funds were disposed of in different provinces within a short period. The funds were all disposed of through ATM cash withdrawals. The change in account behaviour, where the individual no longer disposed of funds through card purchases and electronic funds transfers, were seen as an indication of a kidnapping activity. The transactional activities noted in the account reflected the movement of funds as rapid in and out within a short period.
- Suspicious activity was identified in a director's business account. The director was allegedly kidnapped and the perpetrators demanded a ransom from the director's friends and family members. The accountable institution noted multiple cash withdrawals from the business account at night at different outlets, which was deemed suspicious and unusual.

Illicit financial flows

- An accountable institution reported suspicion of illicit flow of funds following multiple incoming and outgoing of funds over a short period. An individual's personal account reflected 22 transfers to other accounts amounting to millions of rand. The transactional activity as well as the profile of the individual did not match the transactional behaviour identified in the account.
- Multiple cash deposits in rounded amounts were made into an individual's account referencing individual names. The suspicious transactions were coupled by international ATM cash withdrawals, which was deemed unusual and suspicious for an individual account.

Third-party transactions

- Regulatory reports were filed flagging a possible third-party transaction linked to potential illicit flows of funds and fraud. The accounts reflected multiple high-value credits which the accountable institution deemed suspicious. The accountable institution was subpoenaed on the account for the alleged fraud. The account also received funds through electronic transfers, which were disposed of quickly after receipt through electronic payments to third-party beneficiaries.
- Multiple suspicious cash deposits from unknown sources were made into the account of an individual without justification for the number of transactions. The behaviour was reported for possible abuse of the account as well as a possible third-party transaction where the account was used as a mule to facilitate transactions on behalf of an unknown party.
- Business accounts belonging to foreign nationals received funds alleged to be from the proceeds of crime. The accountable institution suspected the funds were the proceeds of a crime from a third party implicated in fraudulent activities. The funds were subsequently dispersed through several outgoing electronic transfers to multiple accounts.
- Suspicious structured high-value amounts were deposited into a business account. The depositor could not provide details of the source of funds. The funds were disposed of through transfers.
- A business account received multiple, large third-party cash deposits, which were deemed suspicious, from government-owned entities. The funds were disposed of through debit transfers, debit card purchases, immediate payments, and internet banking transfers. It is alleged the account was opened for defrauding accountable institutions and government entities.

Foreign exchange agents transactions

- The commonalities among entities included the same e-mail address and the authorised signatory who did not seem to be the ultimate beneficial owner or the director. The transactions also had the same beneficiary based in Taiwan dealing in various goods. The Taiwanese entity did not have an online footprint which may have pointed to the existence of a shell company. One of the source entities identified in the regulatory reports traded in hemp products (face masks) since 2020. The source entity had made payment of over R21 million for imported face masks. This information was reported by an accountable institution.
- Foreign exchange agents or companies also reported suspicious transactions that involved entities registered on the same day with the same address and beneficial owner. Another suspicious transaction between the two companies included payments of R83 million within eight days for the purchase of face masks. The accountable institutions could not ascertain the source of funds and the reason for the beneficial owner registering two businesses of the same nature and transacting high-value funds between the entities days apart.

Profiling of money mules as seen in regulatory reports

Money mule profile



MALE

71% male perpetrators

Male perpetrators were signatories in companies across multiple sectors



SECTORS OF COMPANIES OWNED BY PERPETRATORS

Cash and carry (27%)

- Construction (11%)
- Engineering (90%)
- Construction and maintenance (5%)
- Retail (5%)
- Mining (2%)
- Guest house (2%)

ACCOUNT TYPE

Current account (28%)

- Business account (25%)
- Transmission account (23%)
- Cheque account (12%)
- Unknown account (8%)
- Retail forex account (2%)
- Bizlaunch account (1%)
- Money market account (1%)



NATIONALITY

- Mozambique 2%
- Ghana 9%
- Unknown 9%
- China 9%
- South Africa 71%**

AGE	POPULATION %
21 - 30	24%
31 - 40	0%
41 - 50	41%
51 - 60	26%
>61	9%



FEMALE

29% female perpetrators

Female were often identified as unemployed, signatories and directors in companies across multiple sectors



SECTORS OF COMPANIES OWNED BY PERPETRATORS

Cash and carry (15%)

- Consultants (45%)**
- Household (7%)
- Catering and Construction (5%)
- Guest house (4%)
- Plumbing services and printing (2%)

ACCOUNT TYPE

Current account (31%)

- Business account (11%)
- Transmission account (29%)
- Cheque account (17%)
- Unknown account (10%)
- Retail forex account (2%)
- Bizlaunch account (1%)



NATIONALITY

- Mozambique 2%
- Unknown 27%
- China 15%
- South Africa 56%**

AGE	POPULATION %
21 - 30	7%
31 - 40	61%
41 - 50	20%
51 - 60	6%
>61	6%

Table 4: Characteristics of reported persons or entities and transacting patterns in STR reports linked to money mule cases

Characteristics	Trend
Nationality	Persons identified in cases were primarily South African (61 percent), unknown (22 percent), Chinese (12 percent), Ghanaian (four percent), and Mozambican (two percent).
Gender	The majority (71 percent) of individuals linked to money muling in the STR data mining involved men.
Occupation	Perpetrators linked to money muling related activities included directors, signatories and unemployed individuals. Many of the regulatory reports analysed did not provide information regarding occupations.
Business used	The following business types were noted in cases relating to money mule activities: <ul style="list-style-type: none"> • Manufactures • Importers and exporters • Stockists of pipes, flanges, pipe fittings, bolting and general engineering for the oil, mining, and petrochemical industries • Consultants • Catering • Construction • Transportation • Civil works • Engineering • Tent and chair hire, and other related activities • Retail in second-hand goods • Cash and carry • Motor vehicle dealership • Warehouse • Steelworks • Hardware
Account activity	Indicators relating to accounts included: <ul style="list-style-type: none"> • Business accounts not displaying expected business expenditure such as salaries and tax payments • Personal accounts reflecting salary credits, living expenses and debit orders and high-volume and value EFTs • In many cases there appeared to be a rapid disposition of funds after receipt through cash withdrawals, electronic transfers, and international cash withdrawals • Inability to confirm source of funds or wealth • South Africans • Newly opened accounts as well as shelf and shell companies that were previously dormant suddenly credited with high-value amounts from government-owned entities.
Transaction mode	Transaction modes related to money muling were: <ul style="list-style-type: none"> • Electronic funds transfer • Cash payment • ATMs • Money remittance • In-branch cash deposits • Forex transactions • Point of sale • Telegraphic transfers

Characteristics	Trend
Source of wealth	The source of wealth noted for alleged perpetrators included: <ul style="list-style-type: none"> • Unknown • Magtape credit • Real-time transfer • Cash deposits • Cash withdrawal at ATMs • Credit transfer
Convictions	No convictions were noted in regulatory reports related to money muling for the period under review
Deposit references	Deposit references linked to suspected money mule transactions often included random names: "Maintenance"; "BANK ADJUSTMENT"; "DR"; "DRC TRIP COSTS"
Political exposed persons	No politically influential persons were identified in the regulatory reports

Authorised dealers in foreign exchange with limited authority

Authorised dealers in foreign exchange with limited authority (ADLAs) are authorised by the Financial Surveillance Department of the Reserve Bank to deal in certain foreign exchange transactions which include *bureaux de change*, independent money transfers and value transfer services.

ADLAs are often vulnerable to being targeted for money laundering, terrorist financing and other predicate crimes. The globalisation of the financial sector and the development of sophisticated information technologies has contributed to a considerable increase in the volume and value of the transaction activity carried out by ADLAs.

Money remittance, foreign exchange agents and travellers' cheque transactions were identified in the STR data mining exercise.

Structuring or "smurfing" was frequently reported and appears to remain the most usual money laundering method identified in the ADLA sector. Structuring occurs when a person carries out several cash transactions by breaking them into smaller amounts to avoid the mandatory threshold reporting and/or customer identification requirements. Such transactions may be carried out in a single day or over a period, through the same or several agents.

Indicators for all ADLA service provider categories as identified in the regulatory reports linked to cases:

Characteristics	Indicators
Transactions	<ul style="list-style-type: none"> • The transaction seems to involve complexity • Use of possible fronts and/or shell companies • Transactions in a series are structured just below the regulatory threshold • The customer appears to be trying to avoid reporting requirements by using two or more service providers, locations or cashiers on the same day to break one transaction into smaller transactions • Frequent transactions made by the same client with no apparent purpose or no obvious economic or financial basis • Sudden increases in the frequency or value of transactions of a particular customer without a reasonable explanation • The transaction is unnecessarily routed through third parties • Customer sends or receives funds to or from him/herself for no apparent purpose through mobile money transfer top-ups • Customer sends or receives funds to or from counterparts located in jurisdictions which are known to be exposed to risks of drug trafficking, terrorism financing, smuggling etc.









Characteristics	Indicators
	<ul style="list-style-type: none"> • Customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or difficult for the ADLA to verify • No or limited information about the origin of funds • Customer is accompanied by others who keep a low profile or remain just outside the ADLA's premises • Customer reads from a note with sender information that is not written by themselves • Customer appears to be in doubt when asked for further details regarding the transaction(s) • No apparent relationship between the sender and beneficiary • Sudden increases in the frequency or value of transactions without a reasonable explanation • Funds are sent at a time not associated with salary payments • Remittance sent outside migrant remittance corridors • Cash is in used notes and/or small denominations (possible indication that the money originates from a criminal offence) • Customer refuses to disclose the source of cash • Exchange of large quantities of low denomination notes for higher denominations • The customer buys currency that does not fit with what is known about the customer's destination • The customer acts suspiciously, and does not watch the counting of money • Use of different money remittance businesses
Customer profile and behaviour	<ul style="list-style-type: none"> • Customer's area of residence is inconsistent with other profile details such as employment • The size or frequency of transaction(s) is not consistent with the normal activities of the customer or the expected transacting behaviour • Many persons are registered at the stated address, or there is a large number of changing occupants, or other information available indicating that it is not the real address of residence or domicile • The customer is unwilling to provide details of his/her identity information and references • Use of false identity documents to send money • The customer shows no interest in costs or interests rate charges regarding the transaction.

Crypto asset service providers

A crypto asset is defined as a digital representation of value that is not issued by a central bank, but is traded, transferred, and stored electronically by natural and legal persons for the purpose of payment, investment, and other forms of utility, and applies cryptography techniques in the underlying technology. Crypto currencies can function as a medium of exchange, unit of account as well as a

store of value, however, they do not qualify as a legal tender within any jurisdiction. Crypto currencies are not illegal and are often used by consumers as a form of payment owing to their highly secure nature, as well as their fast transferability. Criminals exploit these benefits to further their illicit activities in predicate crimes, money laundering and terrorist financing.

Indicators of illicit financial flows identified during the STR data mining linked to crypto asset service providers:

	Large flow of funds credited into the bank account over a short period
	Clients unable to provide details regarding the source of funds
	Client receiving numerous internal transfers from other banking institutions followed by rapid disbursement via external transfers with the name of a crypto exchange in the description
	Recorded expected monthly salary does not correspond with the client's profile and transaction history
	Clients making use of personal banking accounts for business purposes
	High-value fiat deposits made in short periods
	High-value daily cash deposits followed by rapid transfers to CASPs
	Individual accounts not engaging in normal banking activities where funds are moved out of the account through CASPs
	Bank accounts not maintaining a high balance due to rapid depletion of funds
	Funds received via large EFT payments from various accounts as well as numerous cash deposits as source of funds
	Unknown nature and purpose of cash transactions

Suspicious transaction trends identified in the STR mining exercise

- The use of shell companies to host fraudulent funds
- South African nationals identified as directors or signatories of entities implicated in money muling or illicit financial flow activities
- South African nationals used to collect money remitter transactions from other jurisdictions with no clear purpose for the use of funds and unknown relation between the sender and the receiver
- High-value electronic credits followed by immediate disposal of funds
- One director of multiple companies who sends funds between the companies.

Qualities of good suspicious and unusual transaction or activity reports

- Correct selection of indicators (the FIC is in the process of supplementing the list of indicators on goAML relating to money mule or illicit financing transactions and activities)
- Grounds for suspicion - Use of specific terms such as money mule or money muling when referring to this crime type or suspicion
- Select the correct report type i.e. suspicious and unusual transaction report or suspicious activity report
- Complete mandatory fields such as the date of birth and identity number (ID) number
- Provide sufficient transactional information when making regulatory reports
- Provide additional information such as occupation of the customer and suspect behaviour, that will assist with intelligence gathering and analysis
- Submit section 29 regulatory reports within the appropriate time frames
- Regulatory reports must contain sufficient information regarding the activity or the transaction between parties in relation to money mule suspicions
- Provide complete and sufficient information on suspected money mule activity
- Provide details of the type of accounts involved in suspected money mule activity.

Locations of money mule activity and regulatory reporting

Regulatory report locations

Accountable institutions often file regulatory reports to the FIC via their head office locations and not where the transaction took place.

It is important to distinguish between locations where money mule activity takes place and from where the reports were filed. Money mule related transactions mainly took place across Gauteng and the Western Cape provinces.

Transaction location

Money mule related activities were concentrated around areas in Gauteng and the Western Cape. Transactions that took place in Gauteng were mainly in Roodepoort, Cresta, Fordsburg and Southdale. In the Western Cape, the areas which had the highest number of reports included Stellenbosch and Cape Town.

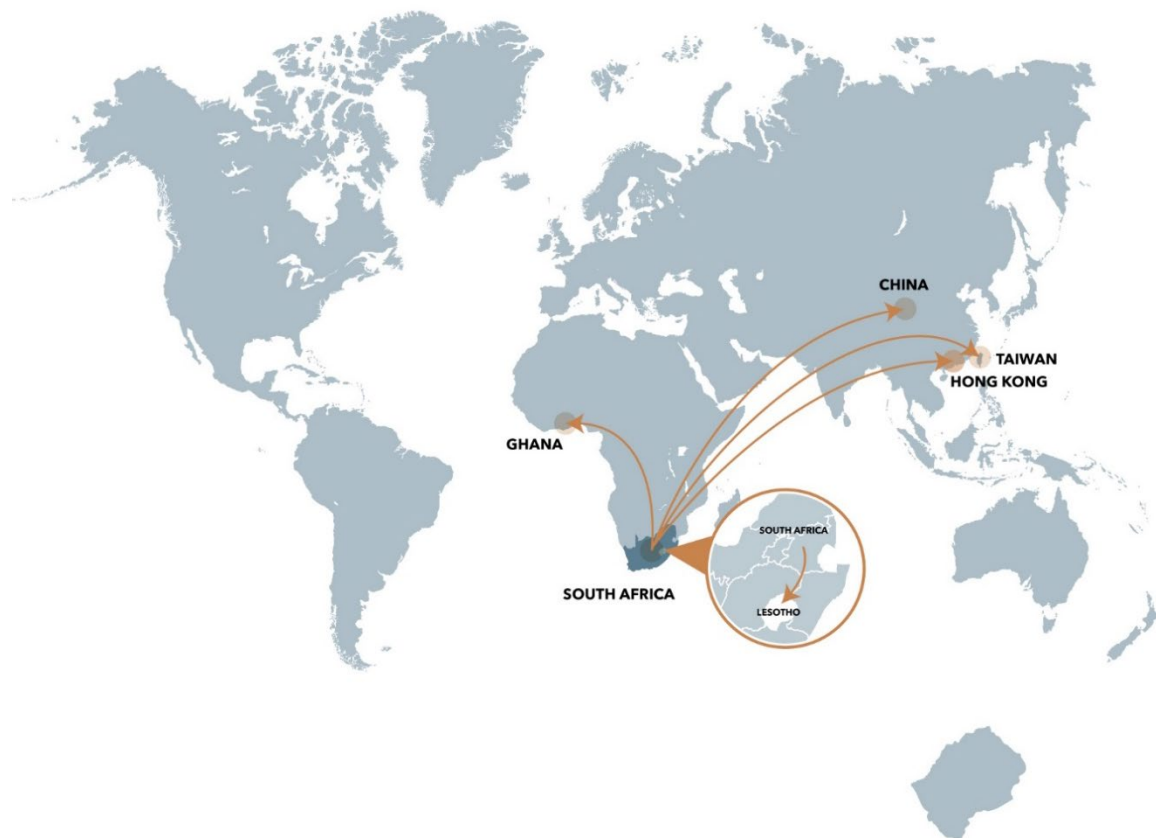
A fair number of regulatory reports were received from other provinces such as Limpopo, the Eastern Cape, Mpumalanga, and the North West.

The FIC encourages accountable institutions to indicate the location where the suspicious transaction took place or at a branch level as this enables more accurate data on indicators and trends.

Outbound transactions from South Africa

Outbound transactions from South Africa were also analysed during the STR data mining process. Most of the funds leaving South Africa were transferred to China, Ghana, Hong Kong, Taiwan and Lesotho, in no specific order. Some of these transactions for funds leaving South Africa were related to cross-border money remittances.

Figure 4: Outbound cross-border transactions from South Africa



Conclusion and recommendations

The STR data mining analysis provided insights into the available intelligence about money muling, the main actors and business entities involved. Also highlighted were the gaps in reports which did not shed light on the ultimate beneficial owners in these crimes.

Reported transactions linked to money muling and the illicit flow of funds were limited in terms of explaining the grounds for suspicion and providing sufficient information regarding the details of the persons, accounts or entities involved. Some of the regulatory reports were filed based on adverse media coverage, subpoenas, and section 27 reports (defensive STR). The reporters often suspected suspicious transactions or activity in a client's account but provided no corroborating evidence on aspects such as source of funds or purpose of transactions or to report the crime as money muling.

The data mining showed that crypto currency transactions in relation to illicit financial flows crimes were relatively high. This evolving technology is increasingly popular among criminals and should be monitored for future trends. The money remittance sector should also be closely monitored, especially since large volume of funds enter and

leave the country via these services. Transactions in the money remittance sector is largely cash based, although other payment methods are used to facilitate the transactions.

Close attention should be paid by casinos as many regulatory reports relating the sector were identified during the data mining exercise where a suspicion of possible runners or mules facilitating transactions were identified.

Banks recorded the highest number and value of regulatory reports relating to the suspicion of possible money mule activity. With huge volumes of transactions and cash flowing through the banking system daily, banks remain the biggest reporters and usually provide much information regarding a suspicion.

Information provided by other accountable institutions is sometimes insufficient regarding transactional information, grounds for suspicion as well as details regarding the occupation of their clients.

Locations for suspected money mule activity

The location where predicate offences, often sponsored by money muling, occurs tends to be different to the residential addresses of suspected perpetrators.

How to address money mule activities:

- Develop initiatives to increase victim reporting and enhance suspicious transaction reporting
- Effectively analyse voluminous information primarily those below the reporting threshold and the high-value inflows to tackle money mules
- Adopt strong domestic co-ordination mechanisms between the public and private sectors to holistically address this crime.

How institutions can help stem money muling:

Closer collaboration between accountable institutions and authorities may assist in obtaining richer data regarding perpetrators and their activities, and ultimately identify the proceeds of crime, and criminal behaviour faster and more accurately. The creation of joint working groups where reasonable suspicion of money muling exists may shed light on certain customer behaviour, employment type, source of funds and may assist in producing actionable financial intelligence.

Case studies

CASE STUDY 1 - FRAUD



An STR was reported on a subject whose account received funds via electronic payments and cash deposits. The funds were disposed through electronic payments, cash withdrawals, debit orders and point of sale purchases. The transactional conduct did not appear to be entirely forthcoming as the unknown reporter could not confirm whether the funds were obtained legitimately. The account was cash intensive, which posed a money laundering risk due to the high risk associated with cash. The illicit flow of funds was suspected as the funds were moved shortly after receipt.

Analysis of financial and crypto statements revealed large credits into the subject's accounts which were converted into crypto currency and disbursed from the account. The source and purpose of the funds were unknown. With consideration to the financial profiling and conduct, the unexplained income and suspicious transactions linked to the subject, the FIC could not rule out illicit or unlawful activity. The FIC shared the financial analysis and intelligence with law enforcement.

Multiple STR reports were received for the subject indicating the following:

- Large fiat deposits made into a crypto currency exchange account
- Funds were rapidly depleted once large deposits were made daily. It appeared that the subject was hasty to transfer the funds out of the exchange
- Cash threshold reports were submitted on round amount deposits made to the subject's account.

Analysis of statements revealed the account was largely credited via electronic credits that contained references to vehicles, hair salon type business, salary, loan, and individual name references. The contra account details showed funds originated from various accounts in one bank. The funds in the account were debited mainly to the crypto asset exchange. From the account overview, it appeared that the subject may have been using the account to conduct business transactions. The disbursement of funds to a crypto asset exchange in large quantities raised suspicion as to the source and legitimacy of the funds.

From the transactional overview, the crypto asset account received a large amount of fiat deposits into the account that appeared to be used for crypto currency purchases mainly in the crypto currency XRP. The crypto currency appeared to be sent to addresses in the name of the two bitcoin exchanges. The source and purpose of the deposits and subsequent conversion to crypto currency were unknown and may have originated from unlawful sources. The conversion of the fiat currency to crypto currency may have been an attempt at layering illicit funds.

The subject was listed as unemployed but received numerous cash credits into the account while the source of funds was unknown. The activity in the account did not match the profile and the cash credits exceeded the threshold amount.

From the account analysis, the account was credited predominantly via cash deposits and internal credit transfers. The deposits were made in rounded amounts almost monthly into the account. Due to the nature of cash transactions, the source and purpose of the cash deposits were unknown and may have been derived from unlawful activity. The second largest contributing credits to the account was via inter account transfers to various account holders. The relation between the account holders and the subject was unknown and the purpose for which these credits were received were unknown.

The reasoning for transferring funds to the account holder was unknown and may be linked to unlawful activity. The transactions took place in the month of December 2022. It could not be ruled out that the subject may have played a role in layering funds or her account may be used as a mule account. With consideration to the financial profiling, financial conduct, unexplained income and suspicious transactions linked to the subject, the FIC could not rule out the possibility of illicit or unlawful activity.

CASE STUDY 2 - TAX REFUND FRAUD



The FIC received a suspicious activity report from a bank relating to clients who received fraudulent refunds from SARS on 19 and 20 April 2023. The subjects received tax refunds ranging from R30 000 to R39 000. Most of the subjects were from Mpumalanga, and upon further investigation the reporter identified that the SARS refunds may be part of a scam referred to on social media as "Wara Wara".

Ninety-one subjects were reported of whom 78 resided in Mpumalanga, while the other 13 lived in Gauteng, KwaZulu-Natal, and the Eastern Cape. While both online and in-branch methods were used for the onboarding process, it was noticed that two branches in Mpumalanga seemed to be the most preferred for subjects who onboarded in person. The rest of the subjects used various other branches. Twenty of the subjects onboarded either online or used the bank's application. Their preferred branch could therefore not be established.

While all the subjects had accounts with the reporting bank where they received the suspected fraudulent SARS refunds, they also held active and inactive profiles with other banking institutions.

Open-source data collected by the FIC pointed to groups on social media under the "Wara Wara" scam aimed at luring individuals interested in receiving funds from SARS by submitting fraudulent income tax claims. The *modus operandi* of this crime included convincing members of the public to reveal their personal information to the perpetrators, including e-Filing usernames and passwords, which are then used during the tax submission and claiming process. The claimants received approximately R40 000 into their bank accounts after which a portion of the funds were paid to the perpetrators. Open-source data showed in some instances that members of the public could use the same details to receive a refund from the revenue service on multiple occasions.

The FIC's open-source analysis identified several role players who hosted some of the "Wara Wara" sites and whose details were provided in the disseminated reports.

A South African Anti-Money Laundering Integrated Task Force tactical operations group looking at fraudulent tax refunds has been established.

CASE STUDY 3 - ILLICIT FINANCIAL FLOWS



A subject, through her linked entity, was alleged to have provided loans to individuals. In exchange they would open bank accounts in their names and hand over to the subject their personal bank cards with linked PIN numbers. The subject was suspected of using or facilitating the accounts for money muling activities and potential money laundering and/or moving funds illicitly outside the country. Cash withdrawals were made in China. The subject was linked to an illicit financial flow scheme involving multiple Chinese role players, using mule accounts to launder funds suspected to have originated from illegal activities. The relevant regulatory bodies were alerted to the involvement of the subject in an illicit financial flow scheme.

Financial intelligence revealed that the subject was the sole director of the entity under suspicion and had no significant financial footprint in South Africa. Multiple suspicious transaction reports were received for the subject. Her linked bank accounts were reported to have received funds via multiple large electronic transfers, which were rapidly disposed of via various card purchases and electronic payments soon after receipt. Reporters could not establish the sources and legitimacy of the funds while the transactional activity was not in line with the subject's profile. Despite the subject being listed as employed, no salary was evident in her account.

Financial analysis revealed that the credit turnover on the subject's accounts was inconsistent. The business account of the subject's entity was predominantly credited via large, rounded amounts of electronic transfers that were referenced in various individuals' names and originated from multiple accounts. The account numbers were mainly held in the name of various business entities linked to Chinese individuals. The funds were subsequently disposed of via card purchases and electronic payments almost immediately after receipt. The funds in the account were mainly dispersed via multiple electronic transfers to various individual accounts linked to Chinese nationals. It was noted that large outward cross-border transfers were made from the account to China. The frequent cash withdrawals in China were made with no apparent business purpose or reason. The subject was reportedly in South Africa at the time of the withdrawals and the withdrawals were made in amounts that were below the reporting threshold.

Account analysis confirmed unusual and suspicious transactional activity as reported. The receipt of funds from various sources and the rapid disposition of funds, notably the frequent cash withdrawals in China were of concern, as these were made reportedly while the subject was in South Africa. During analysis it was noted that the subject had financial interactions with another known subject of an identified illicit financial flow scheme. Analysis indicated the operation of an illicit financial flow scheme and appeared to have contravened exchange control regulations while the funds are suspected to have been obtained unlawfully.

CASE STUDY 4 - ILLICIT FINANCIAL FLOWS SCHEME



An illicit financial flows scheme was uncovered in 1 495 transactional activities involving 320 individuals to the value of R80 681 469.28. The accounts showed similar activity with unusual turnovers over a six-month period. New crypto asset accounts, funded in a manner inconsistent with the owner's customer profile and financial standing, were detected. Frequent transfers of large amounts of crypto assets within a set period (day, week, month) to the same account from various individuals and transferred immediately.

- The FIC became aware of the scheme through a regulatory report filed by a crypto asset exchange provider
- The client exhibited unusual transaction features with turnover of R11 million over a month
- Transactional activity on the crypto wallet indicated that the account was funded by various account holders who were possibly money mules from one institution
- Opening documents provided included fabricated bank statements
- New bank account was opened, and sum of R1 214 336.71 was transferred from a crypto wallet to the new account
- Urgent follow-up engagements were held with the bank and SARB to advise on matter. Open-source data indicated funds were transferred to foreign jurisdictions.

The combined effort of the stakeholders in the tactical operations group assisted in identifying the top-20 transactors with unique reference numbers linked to crypto wallets and bank accounts linked to all parties involved in the financial crime. Due to the complex nature of the transactional activity, the analysis and engagements between regulatory authorities and law enforcement continue as multiple parties have been identified.

References

Barclays:

<https://home.barclays/news/press-releases/2023/10/barclays-warns-of-23-per-cent-surge-in-student-money-mules/#:~:text=2nd%20October%202023%3A%20Barclays%20is,a%20type%20of%20money%20laundering>

Corruption watch:

<https://www.corruptionwatch.org.za/interpol-raises-awareness-of-the-role-of-money-mules-in-the-criminal-cycle/>

Daily Maverick:

<https://www.dailymaverick.co.za/article/2023-05-17-gen-zs-from-joburg-the-most-susceptible-to-money-mule-recruitment-stats-show/>

Financial Action Task Force:

<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering-Executive-Summary.pdf>
<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf.coredownload.pdf>

Financial Sector Conduct Authority (FSCA):

<https://www.fsca.co.za/News%20Documents/FSCA%20Press%20Release%20-%20FSCA%20cautions%20consumers%20against%20mule%20bank%20account%20scams.pdf>

International Monetary Fund:

<https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Remittances>

South African Banking Risk Information Centre (SABRIC):

<https://www.sabric.co.za/search-results/?q=MONEY+MULES>

South African Fraud Prevention Service (SAFPS):

https://www.safps.org.za/Home/FraudPrevention_TipsAndTraps

South African Revenue Service (SARS):

<https://www.sars.gov.za/targeting-tax-crime/what-is-a-tax-crime/sars-and-the-criminal-justice-system/>

Trustfull:

<https://trustfull.com/articles/how-to-spot-money-mule-red-flags-in-banking>



Financial
Intelligence Centre