

The seal of the Financial Intelligence Agency, Bermuda, is a circular emblem. It features a blue outer ring with the text "FINANCIAL INTELLIGENCE AGENCY" at the top and "BERMUDA" at the bottom. Inside the ring is a yellow field containing a blue silhouette of the island of Bermuda. The text "SELECT FINANCIAL INTELLIGENCE AGENCY CASE STUDIES" is centered over the seal in a bold, black, serif font.

**SELECT
FINANCIAL INTELLIGENCE
AGENCY
CASE STUDIES**

1st Quarter 2019

INTRODUCTION

The Financial Intelligence Agency (FIA) is Bermuda's Financial Intelligence Unit (FIU) and was established, in part, to meet recommendations of the Financial Action Task Force, including FATF Recommendation 29 whereby:

“Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly. ”

In carrying out its functions, the FIA collects Suspicious Activity Reports (SAR) from regulated entities and others related to money laundering and terrorist financing as required under Bermuda's Proceeds of Crime Act (POCA).

As part of its FIU functions, the FIA then analyzes the data provided via SARs to uncover activities and patterns that may indicate money laundering, terrorism financing or other related criminal activities. This information is then disseminated as intelligence to local law enforcement and regulators as well as certain international partners.

CASE STUDIES AND INDICATORS

The FIA analyzes hundreds of SARs each year and based upon this information produces dozens of intelligence disclosures each quarter to its local and international partners. The case studies contained in this report are sanitized and representative examples of intelligence cases disclosed by the FIA. As part of the FIA's commitment to the fight against money laundering, terrorist financing and related crimes, the FIA produced this report of case studies to assist reporting entities in identifying and reporting suspicious activity to the FIA.

In general terms, case studies are an analysis of persons, groups, and events which are studied to find underlying principles. The FIA selected the following from reports recently provided to the FIA and analyzed for the 1st quarter of 2019

The FIA has also identified indicators of money laundering / terrorist financing within the case studies. These indicators are generalized underlying principles that have been found by the FIA and our international partners. A list of common identifiers have been compiled and coded into goAML and when filing a SAR, reporting entities are now able to choose from a list of over 100+ indicators.

In the context of individual case studies, such as those presented in this document, an indicator can be considered a “Red Flag”. Such a Red Flag could then be used by a reporting entity as a basis for suspicion by a reporting entity.

CASE STUDIES

The following case studies illustrate suspicious activity reported to the FIA in the 1st quarter of 2019

2019 FIRST QUARTER

Case Study 1

1. STR filed by a local bank uncovers rogue local gatekeeper

An STR was submitted by a local bank on the suspicious flow of funds between the accounts of a local businesswoman, several senior citizens as well as local and overseas businesses.

A review conducted of the accounts of senior citizen, Mr. T, over a 10 month period in 2018 identified an unusually large international cheque deposited on one of his account in the amount of USD \$25,000.00. Open source searches revealed no information about Mr. T and his international associates. During this 10 month review period, the account in question saw over BMD \$300,000.00 transferred funds to Rosebud Limited and over BMD\$100,000.00 transferred to a local firm, Paz Co. Funds were also seen to be crediting the personal accounts of the owner of Paz Co., Miss Z.

Further review of Mr. T's account saw that a Manager's Cheque was issued to senior citizen, Mr. P, in August 2018 in the amount of BMD\$75,000.00. Although there was no clear reason for the issuing of the Manager's Cheque, it was noted that the common denominator between Mr. T and Mr. P was Miss. Z; both Mr. T and Mr. P are Miss Z's clients and under her receivership. After the Manager's Cheque was deposited into Mr. P's account, funds were then transferred the same day to Rosebud Limited. Further review of Mr. T's products showed that he holds an investment account, which had a BMD \$50,000.00 redemption during the 10 month review period and then, the account showed a sale of all units in the amount of BMD \$150,000.00. Shortly after the sale of all units, Mr. T's account showed a transfer of BMD \$150,000.00 to Rosebud Limited's account. The closing market value in the account was BMD \$17,451.98.

During the 10 month review period, Mr. P's account showed small amounts transferred to Paz Co. and Miss Z's personal joint account.

A review of the accounts held by Rosebud Limited and Paz. Co. showed the following characteristics:

- Multiple company name changes
- Other persons transferred funds to Rosebud Limited and were under receivership arrangements
- Quite a few cheques were paid out to individuals and businesses overseas
- The account balances of persons under receivership showed low balances and inconsistent account activity.

After reviewing the accounts under Miss Z's receivership, it was noted that large structured amounts were being transferred to the personal account of Miss Z and then transferred to overseas companies and individuals. In all of the accounts under receivership, it was noted that the account balances had been depleted significantly since receivership. Due to this activity, Miss Z is now suspected of financially abusing her clients.

Red Flags of Money Laundering:

- The accounts under receivership were held by senior citizens.
- There were multiple company name changes associated with the account activity of Miss Z.
- Cheques were paid out to individuals and businesses overseas for unknown reasons.
- Account reviews showed that the account balances of persons under receivership showed gradually diminished account balances and/or showed inconsistent account activity.
- Funds under receivership were transferred to the personal accounts of Miss Z, some of which were used for Miss Z's everyday expenses.

FOLLOW-UP

Checks of the FIA database identified that none of the Subjects were previously known to the FIA database. And due to the sensitivity of the suspected activity, a spontaneous disclosure was made immediately to local law enforcement for further investigation.

SENIOR ABUSE REPORTING & INVESTIGATION

Senior abuse includes: physical, sexual and psychological abuse, financial exploitation; and physical and psychological neglect when the alleged abuser has a duty to care for the senior (a person over 65 years of age).

How do I report senior abuse?

Refer to this web link: <https://www.gov.bm/senior-abuse-reporting-and-investigation>

What is Ageing and Disability Services?

Ageing and Disability Services (ADS) of the Ministry of Health provides a range of services to address the needs of seniors and persons with disabilities. Refer to this web link:

<https://www.gov.bm/department/ageing-and-disability-services>

Case Study 2

2. SAR filed by local bank about expensive good purchased in Bermuda by African National

Due to unexpected banking activity and as a result, a review of a local jewelry store's bank account was conducted and resulted in the identification of a wire in the amount of USD \$8,750.00 that was received in March 2018. Of note, the wire was received from an African country that is considered to be a sensitive jurisdiction by the bank as it is known for corruption. The wire details identified the ordering customer as the son of an African oil tycoon. Open source information revealed nothing negative about the son of the tycoon; however, it was noted that the tycoon's primary holding company has a large, diversified investment portfolio in refineries and pipelines.

As this transaction was outside of the normal account activity and there was no documentation on file that clearly stated the connection between the local jewelry store and the ordering customer, more details were requested about the wire via the Relationship Manager. An invoice was provided by the local jewelry store, declaring that the payment was for the purchase of an expensive necklace.

Further research showed that there was negative news in relation to the ordering customer's father in 2015.

Red Flags of Money Laundering

- Adverse media was found on the father of the ordering customer.
- The suspect transaction in March 2018 was outside of the normal account activity of the local jewelry store and there was no documentation on the bank's customer file that clearly stated the connection between the two parties.
- The African country has been linked to corruption.

FOLLOW-UP

Checks made by the FIA with the local bank that filed the STR identified that there was a compliance oversight as there was also a December 2017 outgoing wire made by the ordering customer to the local jewelry store, bringing the aggregate amount to USD\$15,560.00.

Unfortunately, the African country associated with the ordering customer is not a member of the Egmont Group, disallowing for the secure handling of all relevant AML/ATF-related intelligence via the Egmont Secure Web. A disclosure was, however, made to Bermuda Police Service for further investigation.

What is the Egmont Group?

The Egmont Group of Financial Intelligence Units was created to provide FIUs around the world a forum to exchange information confidentially to combat Money Laundering, the Financing of Terrorism and other predicate offences. Read more here: <https://egmontgroup.org/>

Which countries are members of the Egmont Group?

A list of Members of the Egmont Group is found here: <https://egmontgroup.org/en/membership/list>

