SELECT FINANCIAL INTELLIGENCE AGENCY CASE STUDIES

1st Quarter 2020

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 2020

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 2020.

2020 FIRST QUARTER

Case Study 1

1. SAR filed by Bank identifies international narcotics ring

According to Mr. T's account opening documentation, he is a successful self-employed owner of a startup that invests in lifestyle app development and he enjoys working remotely from Bermuda. Due diligence checks conducted by the bank also revealed that his source of income and his source of funds are derived from profits earned by his startup.

During the first 2 years after account opening, the account activity was consistent; however, profits from the regular client base were eventually supplemented by large and irregular payments from eight persons with bank accounts in high risk countries. An internal SAR was then filed by a local bank about the sudden inconsistent and unexpected financial activity noted on Mr. T's personal bank account. Further review of Mr. T's account noted that the profiles of eight (8) certain senders in high risk jurisdictions did not meet the account activity of Mr. T.

A second internal SAR was filed by the local bank on Mr. T's credit card usage as Mr. T had made several unusual inquiries regarding the use of his credit card such as the use of cash advances, and increases in credit limit. Further investigation noted that Mr. T was cleverly using his credit card to discretely withdraw funds from his personal account via the use of cash advances. Mr. T even tried to frontload his credit card in order to withdraw funds via ATMs instead of interacting with bank staff.

Due to the irregularities detected on Mr. T's bank accounts, the local bank decided to terminate the continuance of the banking relationship in 2019 by filing a SAR with the Financial Intelligence Agency (FIA). Upon receipt of the SAR, the FIA sent Requests for Information to the respective Financial Intelligence Units located in jurisdictions linked to Mr. T and the eight suspect remitters. Section 16 Notices were also issued and it was identified that Mr. T held an account at another local bank but that account was used primarily for general living expenses. Checks of the Mr. T's travel movements also identified that he travelled to and from Bermuda every other month.

A response received from X-FIU alleged that Mr. T fraudulently claimed ownership of a local gardening store linked to his lifestyle app. Research conducted by the X-FIU uncovered that Mr. T fraudulently used the gardening store as a means of commingling transfers that were derived from narcotic trading and his startup. Two of the remitters of funds to Mr. T named by the X-FIU

are convicted narcotics dealers, ultimately linking Mr. T to this international drug trafficking ring. It is believed that Mr. T received funds from the two senders in X-FIU's jurisdiction and the illicit funds were then incorporated into a legitimate system, Bermuda, commingled with the startup profits to create the appearance of legality. Overseas investigations continue and the two senders in X-FIU's jurisdiction have been charged with wire fraud, money laundering and drug trafficking.

Red Flags of Suspected Money Laundering:

- Excessive money wire transfer payments received from the bank accounts of multiple unknown persons located in multiple countries that have no apparent economic, lawful or business purpose
- Use of fake invoices to conceal movements of transactions
- Use of fake invoices with the names of legitimate companies; however the purported services of the fake invoice and the legitimate companies do not match
- Subjects held residency/citizenship in more than one country
- The source and origin of the funds for the incoming electronic fund transfer payments were not clear
- Inadequate/evasive explanations were provided to conceal unusual/inconsistent banking activity

Here is an interesting paper written by ACAMS about the opioid epidemic in the US and the role of financial institutions:
http://files.acams.org/pdfs/2018/What_is_the_Opioid_Epidemic_B_Nachin.pdf

Case Study 2

2. SAR filed by Investment Service Provider identifies suspected identity theft

After approving an investment account for Mrs. B, within the first month, multiple chargebacks linked to deposits made to the account were noted by the investment service provider. A compliance review noted that Mrs. B attempted to use multiple credit cards from different international banks located in various jurisdictions using different names.

Of the USD$6,000.00 that Mrs. B attempted to deposit, only USD $650.00 was successfully deposited and traded with a loss of $35.00. She then issued a request attempting to withdraw funds to a bank account that differed from the credit card that he used to make the deposit. As a result, USD $615.00 was withdrawn back to the original source and the chargebacks then returned the remaining funds left in Mrs. B's trading account to the original source.

Further suspect activity that was noted was the client displayed IP addresses in two other countries other than her country of residence. Mrs. B explained that this was because she is a frequent traveler, visiting her children and grandchildren.

Due to the fact that the client attempted to make deposits using multiple cards issued in different countries under different names, the investment service provider deduced that there were reasonable grounds of suspicion that Mrs. B may have fraudulently used credit cards to create and maintain trading accounts.

A SAR was then filed with the FIA and Outgoing Requests for Information (ORI) were sent to FIUs in the 9 countries mentioned in the SAR. Most of the FIUs have acknowledged receipt of the ORI and the FIA awaits updates on how best to proceed.

***Of note, a consent request did not accompany the STR filed by the investment service provider as the chargebacks issued by the banks recovered all of the funds deposited in the investment account.

Red Flags of Suspected Money Laundering:

- Use of credit cards from different countries with different names
- Multiple declined deposits using credit cards
- Use of credit cards with different names from the Subject may indicate identity fraud
- Inconsistent account activity as per account opening documentation
- Multiple credit cards may have been used in order to structure investment deposits
- Chargebacks issued by the international banks of declined credit cards may indicate that fraudulent activity took place.

What is a chargeback?

According to Investopedia, "A chargeback is a charge that is returned to a payment card after a customer successfully disputes an item on their account statement or transactions report. A chargeback may occur on debit cards (and the underlying bank account) or on credit cards. Chargebacks can be granted to a cardholder for a variety of reasons.

KEY TAKEAWAYS

- A chargeback is the payment amount that is returned to a debit or credit card, after a customer disputes the transaction or simply returns the purchased item.
- The chargeback process can be initiated by either the merchant or the cardholder's issuing bank.
- Merchants typically incur a fee from the card issuer when a chargeback occurs."

(https://www.investopedia.com/terms/c/chargeback.asp)

Case Study 3

3. SAR filed by Money Service Bureau on Respectable Businessman

One common reason for suspicion identified in SARs filed by Money Service Bureaus is a sender sending amounts via electronic funds transfers that are not commensurate to the sender's monthly salary or their source of funds. In this case, a Suspicious Transaction Report (STR) was filed on the subject, Mr. P, who earns over BMD$100,000.00 per year and can easily verify his source of funds. You may ask why this scenario is suspicious. The answer is the frequency of the transactions and the excessive number of 'small', structured amounts that were sent to multiple recipients in high risk countries in Central America in a short period of time.

Within 3 months of opening his account, Mr. P conducted 50 transactions to approximately 30 persons in 5 Central American countries, totaling $USD $5,000.00. Interestingly, he had also stated on his customer profile form that he would not send more than USD $750.00 per month. Compliance checks conducted by the MSB noted that the recipients of Mr. P were not previously linked to other senders and that some of the recipients received funds in more than one country. Mr. P's reasons for sending were to help a friend, to help a family member and as a gift.

Checks of the FIA database noted that a previous disclosure had been made to the Bermuda Police Service on the suspect activity of Mr. P. It was also noted that Mr. P has many associates, some of whom are known to the Bermuda Police Service, frequent these same Central American countries and have family members in those countries. Thus, it is possible that Mr. P is sending other persons' funds and/or his own funds on behalf of other persons, which brings into question the true source of funds and the reason for sending.

After conducting intelligence analysis, the FIA made disclosures to Bermuda Police Service, H.M. Customs and respective FIUs in the countries of the recipients of funds. The purpose of these disclosures was to make these agencies aware of Mr. P's suspect activity and to encourage the sharing of intelligence about Mr. P, his travel movements and his associates.

Red Flags of Suspected Money Laundering:

- High risk countries linked to money laundering, and drug trafficking were identified
- Inconsistent account activity was noted contrary to the Subject's customer risk profile form
- Recipients were in similar jurisdictions
- Subject is suspected of acting as a smurf, sending funds on behalf of others
- Funds were sent in small, structured amounts in order to avoid detection of the frequency of transactions

To learn about the evolution of smurfing, please refer to the following link:
https://www.acamstoday.org/from-smurfs-to-mules-21st-century-money-laundering/