SELECT FINANCIAL INTELLIGENCE AGENCY CASE STUDIES

3rd 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 3rd 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 3rd quarter of 2019

2019 THIRD QUARTER

Case Study 1

1. A STR filed by a local investment service provider identified identity fraud

A client, Mr. M, opened an account with a local investment service provider (ISP) in September 2019. The client immediately started to attempt to fund the trading account with USD $2,500.00 using an ABC Bank Ltd MasterCard card issued in Country A and ending in x5586. This transaction failed with the response text stating, "Customer has not returned from ACS". This means that the customer did not return from the ACS page of the issuing bank. The ACS (Access Control Server) page is located in the issuer's domain (i.e. the bank). Each card issuer is required to maintain an ACS which is used to support cardholder authentication. A customer then authenticates to this ACS by providing their authentication details such as username and password, and the ACS signs the result as either a success or a failure. Another transaction valued at USD $2,500.00 using an ABC Bank Ltd MasterCard credit card issued in Country A ending in x4953 was successful.

There was one additional attempt but it was abandoned so, no information regarding the attempted transaction was provided.

Before the funds could be traded by the client it was flagged internally for the review of the ISP and upon review there were several questionable issues identified:

- Passport provided as the client's identification document appeared to be fraudulent. The font was inconsistent, misaligned and appeared to be digitally added onto the document. The security elements were also misaligned or partially covered by the photo;

- The bank statement provided as a proof of residence that could not be verified as genuine. There were indications of inconsistent and misaligned fonts;

- Client wrote his address as being in Country A but also put his country of residence as Country B. Then the client later changed it to Country C;

- During a phone conversation with the client, the client noted that they did not want to deposit with via a method that offered additional security checks, i.e. security code sent to the mobile phone for verification of the transaction; and

- The client had the same nature of business, employment position and financial information listed as a group of clients from Country C that were a part of a credit card fraud ring in the previous year.

With the abovementioned concerns, the ISP had reasonable grounds of suspicion that Mr. M was not who he was and that the funds deposited from the credit card were from a stolen credit card. Therefore, the ISP requested consent to return the funds held, USD 2,500.00, to the original source, ABC Bank Ltd credit card issued ending in x4953.

Report Indicators

- Consent Request
- Credit Cards
- False Documents
- Identity Fraud
- Money laundering
- Collusion

FOLLOW-UP

After analyzing the STR, a letter of non-consent was given to the ISP and Outgoing Requests for Information were sent to Country A, B and C as well as two other countries affiliated with Mr. M per his account opening documentation.

Based on the feedback from the overseas FIUs, Mr. M. was linked to a 'ring of fraudsters' was of interest and the identity of Mr. M was used fraudulently to open the policy as the email address provided and the passport provided were linked to two different countries and persons. The successful transaction of USD $2,500.00 was returned ABC Bank Ltd. via a chargeback and thus, the moratorium period of the non-consent ceased.

What is the difference between identity theft and identity fraud?

Review this webpage to find the answer: https://www.lifelock.com/learn-identity-theft-resources-identity-theft-vs-identity-fraud-whats-the-difference.html

Case Study 2

2. A STR filed by a local bank on a declined business opportunity

According to the local bank, the purpose of this STR was to inform the FIA that it has decided to decline the business of company, XL Ltd. and Ms. O, a Caribbean national.

According to documents provided by Ms. O, XL Ltd. is a private company incorporated in Country A in 2017, of which she is 100% ultimate beneficial owner.

Ms. O and XL Ltd. were referred to the local bank by representatives of Company A. In turn, Ms. O had been referred to Company A by a representative of a luxury hotel chain in Country B that is owned by Ink Holdings Ltd, which was acquired by Company A in 2018. Ms. O had apparently expressed an interest in buying the hotel chain and was looking for an account in the Caribbean to facilitate the sale.

After an initial review by the local bank of the referral, it was recommended that the local bank not proceed with processing the application for onboarding. Several of the following irregularities were identified that led to this decision:

- Documents provided by Ms. O appeared to be requesting the opening of a bank account to receive an usually large sum of money (over USD $65,900,000.00) that she intended to use as collateral to borrow further amounts of money to invest in the hotel chain in Country B. This approach was viewed by the local bank as vague and outlandish.

- The corporate identify of XL Ltd. and the sources of funds for the transactions were unsubstantiated. Open source information show that Ms. O is linked to the shipping industry but not much information was found about her professional background. It was, however, found that the registered address provided by Ms. O was that of a mail forwarding service.

- An additional document may have been included by Ms. O with XL Ltd.'s corporate documents to provide the appearance that XL Ltd. has an investor relationship with another international company in order to add credibility to her account opening intentions at the local bank; however, the purpose of the document was unclear.

- The bank documents from the other bank presented multiple flaws such as the use of a discontinued bank logo, spelling and grammatical errors, varying fonts and 'SWIFT' was improperly formatted as 'Swift'. This type of communication did not correspond with what would be expected from a high net worth individual wishing to establish a high value relationship with a new bank.

CONCLUSION

Based on the details above, the local bank had decided to decline the business. Due to the questionable legitimacy of Ms. O's approach, his unverifiable business and the erroneous documents provided, it was believed that this was an attempt to defraud the local bank, Ink Holdings Ltd. and Company A into either entering a lending relationship with Ms. O or providing some kind of endorsement/information that would have been used to obtain credit from another institution.

REPORT INDICATORS:

104 – Declined/Refused Business
23 – Fraud
22 – False documents
126 – Scams - Imposter

What is an ultimate beneficial owner?

The answer can be found in The Companies & Limited Liability Company (Beneficial Ownership) Amendment Act 2017 found here: http://www.bermudalaws.bm/laws/Annual%20Laws/2017/Acts/Companies%20and%20Limited%20Liability%20Company%20(Beneficial%20Ownership)%20Amendment%20Act%202017.pdf

Case Study 3

3. STRs filed by a Money Service Bureau (MSB) on ring of Bermudians sending funds to the jurisdiction in the Caribbean.

Multiple STRs were filed by a local Money Service Bureau on a ring of Bermudians who were sending funds to the Caribbean. The first STR filed in May 2019 stated that upon research from one of its monthly reports, it was noted that a client by the name of Miss. U had sent USD $1200.00 in February 2019 to Mr. Q in the Caribbean, who is also a recipient of Ms. S. It is suspected they are sending funds for each other, and their profiles have been noted for ongoing monitoring.

REPORT INDICATORS:

- First time customer
- Money transfer
- MSB
- Ongoing Monitoring

According to another STR filed by the local MSB in May 2019, Mr. D sent USD $1,150.00 to Ms. Z in February 2019 in the Caribbean. This receiver's name was also in Ms. S's profile. Mr. D had only conducted one transaction, and had not conducted any further transactions to date of this filing. Mr. D's profile is also noted for ongoing monitoring in order to identify if he was colluding with others and/or had a connection to the upcoming carnival.

REPORT INDICATORS:

- Money transfer
- MSB
- Ongoing monitoring

A third STR submitted by the local MSB in July 2019 detailed a West Indian national, Mr. X had sent USD $900.00 to Mr. Q in the Caribbean and a total of USD $1,500.00 via three transactions to Miss H in the Caribbean in February 2019. Of note, Mr. X had been using 2 IDs, one with his full name and another using his middle and last names. No connection was made between Mr. X and his recipients in the Caribbean upon further review.

REPORT INDICATORS:

- Money transfer
- MSB
- Ongoing monitoring

KEY POINTS TO NOTE

- This island in the Caribbean is a high risk country for money laundering.
- During the period of February 2019, four (4) transfers totaling $ 4,750.00 with the following commonalities were made:
    - Same country in the Caribbean
    - Common Recipient – Mrs. S.
    - Bermudian senders

FIA CHECKS

Checks revealed that only one of the Subjects was known to the FIA and the Bermuda Police Service and that she, Mrs. S, has a criminal history linked to the illicit drug trade. Disclosures were made to local law enforcement agencies for their reference.

Which countries are currently on the EU Policy on High-Risk Third Countries? These countries are said to have strategic deficiencies in their AML/CFT regimes that pose significant threats to the financial system of the Union.

Refer to this website: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_781