FINANCIAL INTELLIGENCE UNIT TYPOLOGY REPORT ON FRAUD

Within a Covid-19 Context (March 2019 – February 2021)

TABLE OF CONTENTS

SUMMARY

In June 2021, the FIU carried out an assessment of the Suspicious Transaction/Activity Reports (STRs/SARs) submitted by financial institutions during the period March 2019 to February 2021.

The objective was to examine the prevalence of fraud in the financial services sector within the context of the COVID-19 pandemic. Specifically, our efforts were geared at:

1. Determining if there was an increase in fraud as a result of the COVID-19 pandemic;

2. Determining if there was an increase in the types of fraudulent activity;

3. Extrapolating indicators of fraud for the benefit of law enforcement and financial services regulators; and

4. Providing the financial services community with insight into an area that poses a high money laundering threat in Barbados and so promote the strengthening of policy and control frameworks, where necessary.

Broad findings are captured in this public report with substantive, specific findings redacted for confidentiality purposes.

LIMITATION OF STUDY

The study was based, **solely**, on the FIU's assessment of STRs/SARs for the period March 2019-February 2020 (i.e. Pre-COVID-19) vs. the period March 2020-February 2021 (i.e. during the pandemic).

FINDINGS & ANALYSIS

In addition to the statistical findings noted at Appendix 1, the following came to light:

1.Use of fraudulent documents

The presentation of fraudulent documents (i.e.pay-slips, job letters and identification documents) **both to open new accounts and secure loan financing, was the most recurring fraud typology.**

Twenty-six attempts were made using this method during the first period and 27 in the second period. This resulted in 11 successful attempts totalling $47,000.00 in the first period and 1 successful attempt totalling $2,500.00 in the second period. In many cases verification of documents presented could not be confirmed for the following reasons:

- the contact information was fictitious;
- the customer was unknown to the stated place of employment; or
- the business was closed.

The following discrepancies were also noted by front-line staff:

- Pay-slip computations for income tax and NIS deductions were inaccurate;
- Barbados Driver's Licenses and identification card proved to be false in some instances notably due to

  - a mismatching of the photograph with the individual producing it; and

-the national registration number not being consistent with the established protocol for the identification number sequence.

There were also attempts to use fraudulent utility bills as a means to show proof of address.

The main entities targeted for this type of fraud were as follows, in order of most attempts:

1. CREDIT UNIONS
2. MICRO LENDERS
3. MONEY SERVICE BUSINESSES
4. COMMERCIAL BANKS

In two instances, persons either forged the signature of the owner of the business or gained access to their employer's electronic signature. A further review of the STRs showed that males (63 or 55%), predominately, were involved in the fraud schemes as compared to 35 females (31%). The remaining 14% related to a combination of legal persons.

Demographically, Barbadian nationals made up the majority of persons perpetuating the various fraud schemes. However, nationals of Guyana, Canada, America, the UK, Venezuela and Nigeria were also identified.

Additionally, certain countries were regarded as having some connection with suspected schemes. These included the UK, Japan, Venezuela and the United States of America. A total of $100,000.00 was remitted to the UK but it could not be conclusively established that the UK was in fact, the final destination.

Fraudulent Financial Instruments

There were 14 attempts to cash fraudulent cheques totalling $1,167,694.90 during the first period with 2 being successful totalling $36,206.51. For the second period, there were 5 attempts totalling $334,854.29 with 1 being successful in the sum of $2,000.00. This particular scheme of issuing fraudulent cheques or seeking to gain money from fraudulent cheques, mainly targeted commercial banks with 14 attempts across the 2 periods.

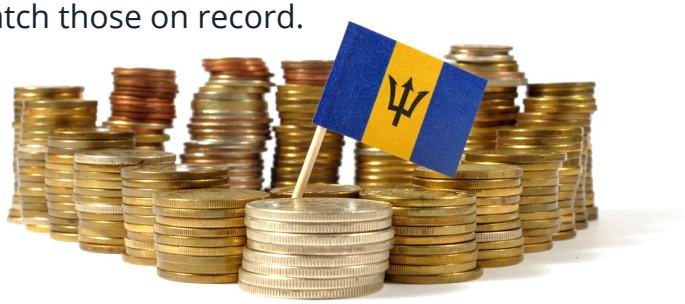
One variant to this fraud typology was 4 instances of cheque kiting that were examined within the two periods. These involved an individual depositing a cheque from their Bank A account, which did not have sufficient funds to cover the cheque, into their account at Bank B. This action created a fictitious balance at Bank B where the individual was able to issue cheques from this account before the original cheque was cleared.

POLICY AND CONTROL WEAKNESSES

Our findings also reflected weaknesses within the policy and control framework of some financial institutions. In one instance, a thread of emails between the financial institution and the purported customer showed that there was a difference in the email address being used by the customer. Additionally, the purported customer submitted three different account numbers to which the funds were to be wired. There appeared to have been no engagement with the true customer either to verify the accuracy of the account numbers submitted, the reasons for the changes, or the authenticity of the transactions.

Policy and control weakness was also observed in the following cases:

- At a commercial bank, an individual was able to withdraw money after a fraudulent cheque, deposited to their account, had purportedly cleared.
- Within the credit union sector, persons were able to withdraw money notwithstanding that the identification picture and signature did not match those on record.



RECOMMENDATIONS:

In light of the noted findings, and with fraud determined as posing a high inherent money laundering threat in the country's financial services landscape (based on the 2019 National Risk Assessment), the FIU put forward a number of recommendations to supervisory and law enforcement authorities.

In addition, financial institutions should pay attention to the following:

1. Understanding the potential (fraud) risk involved in relation to new business initiatives, prior to their roll out, and implement appropriate mitigation measures.

2. Ensuring client-facing and operations staff are kept abreast of fraudulent trends/typologies within the sector through regular training, including cyber-security training.

3. The expansion of customer due diligence measures to include closer scrutiny of documents presented by clients/potential clients.

4. The implementation of enhanced procedures for handling requests for the transfer of funds where instructions are provided remotely (i.e., by e-mail, facsimile, telephone).

5. For board assurance purposes, the implementation of an enhanced audit and/or verification programs; and -

6. The implementation of appropriate internal sanctions for on-going breaches of policies and procedures by employees.

CONCLUSION

According to a FATF report of May 2020 addressing the heightened risk of money laundering and terrorist financing during the COVID-19 pandemic, fraudulent activities had increased as criminals sought to exploit vulnerabilities brought on by the pandemic.[1]

This strategic analysis sought to determine whether, in Barbados, there was indeed an increase in fraud as a direct result of COVID-19. Also assessed were the typologies which emerged during the review period.

Our approach was a comparative one and considered the year prior to the onset of COVID-19 (March 2019) through to its early discovery in Barbados in February 2020 and the period March 2020 up to February 2021 when the pandemic had spread in the island.

From the STRs submitted by the financial institutions and reviewed by the FIU, there did not appear to be an increase in fraud. Neither was their evidence to suggest that the fraudulent schemes perpetrated resulted directly from the presence of COVID-19 in the country.

1. FATF (2020), COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, FATF, Paris, France.

APPENDIX 1

CATERGORIES	MARCH 2019-FEB 2020	MARCH 2020-FEB 2021
# OF STRS/SARS REVIEWED	285	262
# OF STRS/SARS ASSOCIATED WITH FRAUD	67	47
# OF STRS/SARS ASSOCIATED WITH ATTEMPTS TO GAIN MONEY	65	37
# OF **SUCCESSFUL** FRAUDULENT ATTEMPTS	22	8
VALUE OF **LARGEST** ATTEMPTS TO GAIN MONEY	1,200,140	529,624
VALUE OF **SMALLEST** ATTEMPTS TO GAIN MONEY	100	1,000
VALUE OF **TOTAL** ATTEMPTS TO GAIN MONEY	4,818,894	1,411,295
VALUE OF **LARGEST SUCCESSFUL** ATTEMPTS TO GAIN MONEY	218,908	57,900
VALUE OF **SMALLEST SUCCESSFUL** ATTEMPTS TO GAIN MONEY	581	1,000
VALUE OF **TOTAL SUCCESSFUL ATTEMPTS** TO GAIN MONEY	477,641	112,711

APPENDIX 2

1.0 GENERAL

A. On-line approach for business

Indicators

- A request for goods or services is made via on-line or remote means.
- In order to appear credible, the fraudster usually references the names of established or legitimate businesses /organisations.
- The parties involved agree on a sum to be paid.
- A payment is made by the fraudster, using what appears to be an authentic cashier's cheque drawn on legitimate financial institutions.
- The amount of the fraudulent cheque is well in excess of the agreed sum.
- The fraudster then requests the excess be refunded via wire transfer.
- The request for transfer of funds is usually made via email.
- The banking instructions at times have missing information.

B. Business e-mail compromise

Indicators

- The fraudster initiates contact remotely.
- The fraudster uses a close version of the true client's e-mail address to communicate with the financial institution.
- The financial institution does not have clear procedures for handling transactions initiated on a remote basis.

- There is lack of vigilance of client-facing staff;
- Different wire details are provided for the same transaction; or
- Wire details are sent on several occasions via email for the same transaction; or
- There are errors in the wire details.

C. Collusion with outsiders to commit fraud

Indicators

- Centralised decision-making power;
- Lack of accountability mechanisms;
- Lack of separation of duties;
- Mis-representation of facts to exact fraudulent proceeds;
- Creation of false job letters;
- Creation of fraudulent pay-slips;
- Date of the job letters presented out of sync with supporting documentation.

D. Presentation of fraudulent documents to secure loan financing

Indicators

- Job letters are inauthentic
  -There is poor language facility;
  - A false letter-head is used;
  -Stated earnings do not comport with the individual's job title
- Job letters presented are out of sync with supporting documentation.
- The NIS calculations recorded on pay-slips are inaccurate.

2.0 OTHER SUCCESSFUL TYPOLOGIES OBSERVED

EXPLOITATION OF CONTROL WEAKNESSES

A. Review/Clearance Procedures

Indicators

- A fraudulent financial instrument is deposited by the customer at the ATM;
- The fraudulent instrument is held by the financial institution pending clearance procedures;
- The fraudulent instrument is processed after the hold expires;
- The fraudster utilises the fraudulent proceeds through cash withdrawals and POS purchases.

B. Abuse of products and services

Indicators

- The customer secures vehicle financing;
- The customer pawns the vehicle, unknown to the financial institution, who has a lien on the asset pending repayment of the loan.

Indicators

- The customer receives an email requiring the clicking on a link and the entering of a code to activate an account;
- The customer complies with the "instructions";
- Sometime later the customer observes an unexplained withdrawal from their account;

- The client's funds are withdrawn via internet banking by a customer of the same financial institution.

IDENTITY THEFT

A. Third Party Solicitation

Indicators

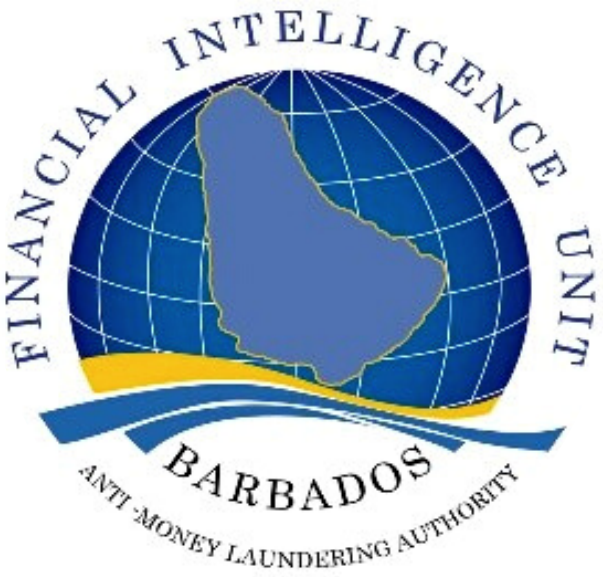
- A customer is contacted, by telephone, by someone, claiming to be a friend living overseas.
- The friend wishes to borrow money promising to repay, with interest.
- The customer agrees and is given the name of a local designate.
- The customer withdraws the money for collection by the local designate.
- The customer's debit card and personal identification number (PIN) are handed over to the local designate.
- The local designate utilises the card to make ATM withdrawals.
- The customer later learns the overseas friend is, in fact, deceased.

B. Personal

Indicators

- An unauthorised individual presents the client's ID card to conduct an over-the-counter transaction.
- The transactions are executed at a particular period during the day, at different branches.

- The Barbados identification card is used to complete the transactions.
- The perpetrator's signature does not entirely match that of the true customer.
- The transactions are executed.



This report is a product of the Barbados Financial Intelligence Unit. This document is intended for informational purposes only and is under no circumstances intended to be used or considered as financial or investment advice.