MONEY TRANSFER AGENCIES

TYPOLOGY

2016-2018

Publication date: February 2019

Author: FIU-Guyana

Table of Contents

ABBREVIATIONS

AMLCFT	Anti Money Laundering and Countering the Financing of Terrorism
ATM	Automated Teller Machine
CFATF	Caribbean Financial Action Task Force
FATF	Financial Action Task Force
FT	Financing of Terrorism
GYD	Guyana Dollar/ currency
ML	Money Laundering
MSB	Money Service Business
MTA	Money Transfer Agency

INTRODUCTION

Globalization of financial services and the financial sector facilitated by rapidly advancing technology has resulted in the movement of funds across the world via Money Transfer Agencies (MTAs) to be quite seamless. Money Transfer Agencies, in this context, refer to entities which carry on the business of transferring sums of money electronically between persons locally and internationally. The speed with which money can be transferred, at relatively low cost, along with the MTAs' accessibility and worldwide reach have made them a viable channel through which funds can be laundered.

Our observation of a sample of MTA data over the period 2016-2018 provides indications that MTAs are being used to create layers of transactions, facilitating the distancing of illicit funds from its source through a series of complex transfers. Sending funds through MTAs, while acting in one's own capacity or as a proxy, affords a criminal an opportunity to place illegitimately acquired money into the financial system; sometimes by direct credit of MTA transactions to accounts of the final recipient.

GENERAL OBJECTIVES

The objectives of this typology are to highlight and provide insight into the ways in which it appears MTAs are being used by launderers to obfuscate the trail of illicit funds with the view of sensitizing operators on the ML risks and vulnerabilities and measures available to them to reduce or mitigate the risks. It also aims to identify trends and patterns, suspected illegal activities, red-flags and modus operandi characteristic of such laundering schemes. Additionally, the public at large can be sensitized about the risks associated with being recruited or used as "smurfs" or "money mules"[1] in the laundering schemes and provide guidance on safeguards they can adopt to protect themselves.

Efforts will also be made to shed some light on the more prevalent predicate offences that are suspected to be associated with the activities observed in transactions processed through the MTAs.

LIMITATIONS OF ANALYSIS

As with activities of this nature, the data and information available to conduct analysis are not always perfect. Despite other minor limitations such as those listed below, the findings of this report are representative of the events and situation in Guyana.

These limitations include:

- **Sample size** – this was influenced by (but not restricted to) data and information gathered by some of the reporting entities

[1] Smurfs or money mules refer to individuals employed in the commission of acts of money laundering e.g. restructuring of amounts transferred or deposited.

- **Reliability and accuracy of data and information** – is, to some extent, dependent on the accuracy & reliability of the data collection systems & methods used by the reporting entities and their ability to spot and report suspicious activities

- **Timeliness and Relevance** – the data used in this analysis is historical information. Methods used by launderers are continually changing and can render analysis on historical information less relevant

Completeness – there is a risk that all relevant information is not obtained by the reporting entities due to the nature of their relationship with the customer.

TYPOLOGY

Criminals seek to hide, move and use funds generated from their illicit activities in a variety of ways, without attracting the attention of law enforcement and other relevant authorities. Structuring and Flipping are two prominent ways criminals use MTAs in laundering schemes. Money Laundering involves three interrelated stages as follows:

- **Placement:** the introduction of cash, which was acquired from illicit sources, into the financial system
- **Layering:** carrying out complex financial transactions to conceal the illegal source of cash by creating as much distance as possible between the source of ill-gotten proceeds and the true beneficiary
- **Integration:** this is the final stage in the money laundering process. It involves reintroducing laundered funds into the legitimate economy while making them appear as though they have originated from a legitimate source.

The two main methods used by criminals to launder funds through MTAs appear to be "structuring" and "flipping" and are defined as follows:

"**Structuring**" refers to the fragmenting or breaking up of a large transaction into several smaller transactions into amounts below the reporting threshold to avoid the triggering of the reporting requirements that are associated with larger transactions, thereby obscuring the trail of funds. Transactions are structured in such a way to not arouse suspicion or attract the usual procedures that are required for larger amounts as prescribed under the AML/CFT Act and Regulations. Sometimes 'smurfs' or 'runners' are used by the launderers to further help with the successful execution of their structuring agenda. Structuring can be carried out in a single day or over a longer period either through the same MTA agent or different agents or locations.

Structuring seems to be the preferred way of laundering funds through an MTA. The presence of several MTAs across Guyana causes structuring to be a relatively easy option for those involved in money laundering schemes as individual agents do not have access to features in the MTA worldwide platform that will allow them to have a global view of customer's activities. This has resulted in mostly reactive action against risky customers after the discovery of suspected illegal activity and the subsequent flagging of customers by a centralized compliance function.

"**Flipping**" can be described as that situation where immediately upon receiving an asset, in this instance cash through a Money Transfer Agency, it is then sent or transferred elsewhere. In other words, it is the act of receiving funds from one source and immediately sending same to another destination. This too, like structuring, is done to "blur" the trail of funds.

Some of the characteristics that make Money Transfer Agencies especially attractive for money laundering are as follows:

- The ease and simplicity with which transactions can be completed,
- Their worldwide reach and accessibility at both ends,
- Their cash-based modus operandi,
- The low cost per transfer when compared with mainstream financial institutions such as commercial banks,
- Less stringent KYC requirements due to non-establishment of a continuing business relationship

Furthermore, the currency exchange which takes place as part of the money transfer seems particularly useful during the placement stage of the money laundering process because such conversion of money renders it more difficult to trace the actual source.

Remittances via MTAs do not necessitate the establishment of an ongoing relationship with the customer, as is the case with the commercial banks; this promotes some level of anonymity which is more convenient for Money Launderers. The electronic databases used by some MTAs to monitor customer behavior and activity enables action to be taken against customers that violate the MTA transfer policy, albeit after the fact.

A formal relationship, requiring standard or enhanced CDD information, is not usually created in the case of MTAs as is done in the banking sector because most transactions with an MTA are classified as one-off transactions. The relationship between the customer and the MTA does not create a situation where there is a vested interest that would compel the customer to maintain that relationship. The customer is usually free to use whichever MTA service he/she pleases on a per transaction basis and is freed of any obligation or interest in the MTA once the transaction is completed. Therefore, the level of monitoring that can be carried out by commercial banks and other entities that maintain a relationship with the customer is different in the case of the MTA. *Launderers have exploited this detached relationship by utilizing many different unsuspecting "smurfs" or "mules" in their laundering schemes*. According to the World Bank Working Paper (No. 163) entitled "The Canada-Caribbean Remittance Corridor" the use of MSBs for criminal purposes seems to be a recurring trend[2].

Through evaluation and analysis of the MTA Threshold Reports and STRs data several Money Laundering red flags have been observed. Many customers, sometimes groups of customers, have been observed conducting multiple transactions on the same day or over a very short time period; very often at the same MTA agents. Most of the observed transactions appeared "structured" to an amount just below the reporting threshold in what seems to be a deliberate ploy by MTA customers to avoid Know Your Customer (KYC) and Source of Funds declaration requirements.

[2] World Bank Working Paper (No. 163) entitled "The Canada-Caribbean Remittance Corridor" -Page 41

Another observation coming out of the analysis is the multiple reports of non-familiarity or lack of evidence to show established relationship between sender and receiver. There are several instances of the customer conducting the transaction being escorted or accompanied by someone who seemed to be more au fait with the intricate details of the transaction and sometimes functioning as a translator.

Suspicious frequency of transfers, inconsistency of transaction amounts with respective customers' profiles, dubious stated purpose of transactions, customers' uncooperative behavior towards MTA agents' requests for information along with the other mentioned observations are all indicators of possible Money Laundering.

MONEY LAUNDERING INDICATORS

Some of the indicators or "red flags" observed in the analysis are as follows:

- Very frequent transactions over a short period of time, usually over a few months.
- A single customer receiving transfers from high number of senders (sometimes from different countries).
- A single beneficiary of multiple remittances in relatively small amounts during a short time period
- Customer appears to be avoiding reporting requirements by using two or more MTA locations or cashiers on the same day to divide larger transactions into multiple smaller transactions
- Several individuals visit the same MTAs on the same day or over several days to send money to the same countries and often to the same beneficiaries; thus, indicating the existence of an organized network desirous of avoiding reporting requirements by breaking large transactions into smaller transactions.
- Transfers are done in small amounts from different MTA agents to various beneficiaries.
- Multiple transfers of equal amounts over a very short period.
- Sums remitted and volume of remittances not in accordance with senders' profiles and are disproportionate to income usually generated by the professions or occupations of customers. This indicates that the senders/receivers may be merely functioning as mules/smurfs on behalf of others.
- Multiple transactions, structured below the regulatory threshold for due diligence checks to same or multiple receivers
- Customer is unwilling to provide routine information when asked by agent.
- None or limited information on source of funds provided subsequent to a request
- Customer is accompanied by others who try to keep a low profile
- Customer reads and must keep referring to money transfer details on a note or cellphone text and seems to be in doubt about the receiver's details
- Customer is receiving instructions from others
- Visible nervousness of MTAs' customers when attempting transaction

SOURCES / ORIGIN OF MONEY:

The increase in the use of electronic means of payments has resulted in greater opportunity for fraud relating to ATMs, credit card, wire transfer, illegal lotteries, advance fee schemes and drug trafficking to name a few. The incidence of such frauds is relatively higher in the developed countries due to the higher adaptation rate of alternative or electronic payment methods when compared with economies where the use of cash remains widespread. Many of the opaque transactions in our analysis are believed to be connected with some of the illegal activities mentioned above.

Criminals' main goal is to obtain the economic benefit from their participation in illegal activities and therefore would seek ways to have the illegal funds legitimized and repatriated to them eventually. Our analysis does not show a preponderance of the same persons receiving funds and immediately, or at a subsequent time, sending money back or onward to another destination. We therefore believe that the remitted funds often change hands physically and are then returned to the original perpetrator through MTA transactions or by other means, e.g. physical transport. The additional layers of transactions render tracing the money an extremely complex task; sometimes, near impossible to resolve.

As regards to remittances from Guyana to destinations such as Colombia, Panama, Dominican Republic and Brazil it is believed that the sources may be locals and illegal aliens predominantly involved in Trafficking in Persons (TIP) and illegal mining. The illegal proceeds are believed to be remitted to family members and associates of those illegal aliens. Reports indicate that gains from Trafficking in Persons, a supposedly highly profitable activity, are also being moved through Money Transfer Agencies in Trinidad and other areas in South America. According to United Nations statistics, human trafficking is considered a highly profitable activity and is becoming the third highest earning criminal activity after trafficking in drugs and arms.[3] In a Financial Action Task Force (FATF) report dealing with money laundering through money remittances, several law enforcement investigations revealed that Money Remittance Service Providers are often used globally as a medium for laundering proceeds from illicit activities such as narcotics trafficking, IT fraud such as phishing, Trafficking in Persons, tax evasion, credit card fraud, advance fee scheme and other consumer fraud.

CASES EXEMPLIFYING STRUCTURING:

I. A few cases where multiple subjects sent multiple transactions to a single individual in the United States of America have been observed. A group of three individuals who each sent identical amounts to the same recipient in the USA was observed. Two of the three senders each remitted money to two other common recipients, in the USA, with common surnames. Approximately GYD$4.M each (USD $20k)- were remitted by these individuals and the transactions seemed inconsistent with their employment profiles. It does appear that these individuals are part of a smurfing network, connected to common recipients in the USA.

II. In June 2018 it was reported that a thirty-eight-year-old customer who sent several transactions to United States of America, the total of which exceeded GYD$ 2.5 M, was unable to provide any information on the source of funds for the transactions. The customer appeared to be operating for or on behalf of a connected third-party. The customers were in the habit of manipulating the surnames and given names (interchanging) of either sender or receiver to prevent the MTA connecting related transactions.

[3] https://www.unric.org/en/human-trafficking

One subject sent six transactions to Nigeria totaling approximately GYD $276K while re-arranging their given name and surname in an attempt to avoid the MTA internal processes detecting the transaction patterns.

III. A case involving several subjects who had received numerous transfers from one sender in the USA was reported. All the recipients visited the MTA agent together to receive the transfers. Some recipients exhibited uncooperative attitudes towards MTA agents when Customer Due Diligence (CDD) information was requested. Those individuals appear to be part of a smurfing network connected to the sender in the USA.

IV. In June 2018 a twenty-six-year-old self-employed individual remitted ten transactions to two receivers in the USA over a period of eight days. This individual could very well be part of a ring that eventually facilitates the return of funds to the original criminal perpetrator.

V. Flagged suspicious transactions sent to Colombia and Dominica Republic where the source of funds and purpose for transfers are unknown:

a) Foreign national sending multiple transactions, each valued at GYD$100,000, from the same MTA location to the same receiver in Colombia.
b) Foreign national sending transactions of identical amount to recipients in Colombia and using multiple agents to avoid being flagged.
c) Several local customers, some with no stated form of employment and some claiming to be housewives, involved in remitting well-structured sums, often of identical amounts, to common recipients in Colombia and Dominican Republic. A subject, with no stated occupation, in one day transferred a total of approximately GYD$700,000 by way of seven equal transactions to one recipient in Colombia.
d) In May 2018 fifteen customers sent transactions to Colombia on the same day. Each of these customers sent between one and three transactions apiece to Colombia and in some instances to a common receiver. Interestingly, values for these transactions were either GYD $96,500, GYD$100,000 or GYD$106,790. These individuals appear to be part of a well-organized network of launderers, structuring transactions to remain inconspicuous.
e) In April 2018 two persons, one claiming to be a taxi driver and the other an employee in the banking/finance sector each sent, at different times on the same day, GYD $159,000 to the same receiver in Colombia.
f) A former employee of an MTA, over a period of eighteen months, sent multiple structured transfers to the Dominican Republic and to the USA. The person who received these transactions from the former employee was also receiving multiple transfers from four other persons, all of whom conducted their transactions at the location at which the former employee was stationed. The former MTA employee received approximately GYD$1.6M in transfers from the USA and the Dominican Republic. On several occasions upon receiving funds from the USA, the subject immediately resends a proportion to the Dominican Republic.

Immediately after certain customers are blocked from using MTAs because of their suspected involvement in smurfing networks, new customers emerge to execute similar transactions thereby continuing the trend.

CASES EXEMPLIFYING FLIPPING

There were a few reported cases involving subjects, entering MTAs, sometimes accompanied by others, receiving transactions from territories such as the USA and Finland and immediately resending similar amounts to jurisdictions like Nigeria and Benin. Nigeria is known for a high incidence of consumer fraud and religious extremism.

a) A subject sent two transfers to two persons in the USA after receiving a transfer from another sender form the USA the previous day.
b) A forty-five-year-old woman who claimed to be unemployed received five (5) transactions from Zimbabwe, each valued at approximately GYD$100k and immediately after receiving each of these transactions, sent a transaction of a slightly lower value to a receiver in Ghana and on each occasion, she claimed that the recipient in Ghana was her friend.
c) In October 2017 a forty- five-year-old female received approximately GYD$40k from a sender in the Philippines and immediately sent a similar amount to a receiver in Nigeria.
d) A thirty-one-year-old female, who claimed to be a vendor, sent transactions to Haiti, Dominican Republic and Colombia over a period of six months after receiving GYD$1.4M in eleven transfers from USA, Cape Verde and Antigua and Barbuda. Business connections to so many jurisdictions are not typical of regular vendors
e) One customer sent a total of GYD$1.8M via forty transfers to Nigeria, some of which were sent immediately after receiving a transfer from the USA.

OTHER OBSERVATIONS

- Multiple transactions sent locally that were initiated by several persons, within the same geographic area, in a short space of time to common recipients in the destination territories.
- Multiple instances of a group of local senders sharing the same residential address.
- Multiple one-to-many relationships between senders and receivers
- Customers suspected to be involved in money laundering transactions mostly indicate the following to be their professions:
    - Taxi drivers,
    - Clerks,
    - Students,
    - Housewives and
    - Employees in the hotel industry
    - Unemployed

  Often, the transactions don't match their profiles
- Most suspected 'smurfs or mules' are between the ages 18 and 40 and are often from the lower income bracket.

RECOMMENDATIONS

- MTAs should explore the possibility of sharing CDD information across the global MTA network concerning blocked and high-risk persons.

- Ensure document retention policy (7 years) is up-to-date and adhered to by all branches/agents and is available across network.

- Strict adherence to the FIU suspicious transaction reporting requirements as it relates to timeliness of reports – STRs should be submitted within three (3) days of forming the suspicion.

- Sensitize customers about the risk of "smurfing" and other ML methods at point of transaction by displaying bold and visible signage that informs them (potential "smurfs or mules") of the possible dangers and penalties of participating in ML and TF schemes if caught. Infomercials in public waiting areas can also be considered.

- Provide continuous training to frontline staff that will equip them with the knowledge and expertise to quickly detect possible cases of ML and TF activities and allow then to take necessary action, including reporting a STR to the FIU.

- Implement pro-active employee screening policy and program that involves ongoing monitoring for employees at all levels including those at the managerial levels.

- Regular training exercises must be conducted by MTAs for employees, officers and agents, with a view to ensuring that they are aware of AML and CFT compliance procedures and the associated legal implications of failing to comply.

- Implement policies and programs to evaluate the effectiveness of the agency's AMLCFT program, especially with respect to the identification or detection of suspicious activity, and ensure timely corrective actions are taken.

- Consider implementing a global end to end transaction flagging mechanism to ensure information is collected on "smurfs" that will facilitate the disruption of the activities of the ML networks and facilitate timely reporting of suspicious activities.

GLOSSARY

Beneficiary	The person who receives the transferred funds/ the person who benefits from an arrangement
Credit card fraud	this is a form of identity theft involving the fraudulent use of someone's credit card information.
Extremism	Having unreasonable and unacceptable beliefs; fanaticism
Financing of Terrorism	this is defined as the provision of financial support to individuals and/or organizations involved in terrorism
Flipping	this is the practice of disposing of an asset immediately after it has been acquired with the intention of obscuring the financial trail.
Illegal mining	refers to the illegal extraction of natural resources without any official or state permission or licenses.
Know Your Customer Requirements	This refers to the process of verifying your customer's identity and assessing potential risks of illegality.
Money laundering	refers to transaction(s) designed to conceal or disguise the true source or origin of illicit sums of money and/or the beneficiary of same. Money laundering involves three stages viz: **1.** ***Placement*** – physically placing illicit proceeds into the financial system **2.** ***Layering*** – distancing the illicit proceeds from the true source by executing a series or layers of transactions to obscure the financial trail **3.** ***Integration*** – the reintroduction of the proceeds into the legitimate economy e.g. by purchasing real estate to create the impression that such funds are "clean"
Money Transfer Agency (MTA)	means an entity, operating as a business, which carries on the business of money transfer for a fee.
Money Transfer	means the making of any payment by a person in the scheduled territory to or for the credit of a person outside the scheduled territory, or to a person in the scheduled territory by order or on behalf of a person outside the scheduled territory**.** (Money Transfer Agencies (Licensing) Act 2009).
Receiver	The person receiving the transferred funds
Scheduled territory	This refers to Guyana
Sender	The person initiating the transfer of funds

Smurfs	**r**efers to individuals employed in the commission of acts of money laundering e.g. restructuring of amounts transferred or deposited.
Tax evasion	this is the illegal underpayment or non- payment of taxes.
Terrorism	this is the illegal use of violence and intimidation being directed especially at civilians with the aim of satisfying certain political objectives.
Trafficking in Persons/ human trafficking	This refers to the movement and exploitation of individuals for the purpose of illicit financial gains