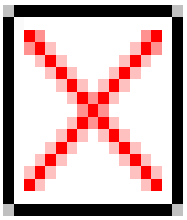
Emergence of new Money Laundering Techniques - A Study

MAY 02, 2022

By L V Rao



HAWALA Channel **1:** ***"Hawala"*** is an Arabic term used for the word 'trust'. Hawala works like a parallel remittance system for transfer of money obtained through unlawful activities and aids money laundering.

1.1 Hawala system of financial transactions were used in Medieval India. The Hawala System does not involve the use of Computers, Cheque Books, Accounts, Book Keeping etc., as visible in the modern banking system. It has also been referred to as ***"Underground Banking"*** . The entire transactions are dependent upon middlemen who are called Hawaldars. The modus operandi adopted in Hawala transaction is unique as there is no real or physical transfer of the funds or monies.

1.1.2

The Hawaldar who took up the responsibility of money transfer for a pre-agreed commission, gets in touch with another Hawaldar in the area where the money is required to be delivered. To receive or collect the money, at the other end, a currency note number or a codeword/password is communicated to the transferee as well as to the Hawaldar located at the recipient place by the sender of the monies. For delivery of cash, the code word/password or the currency note number need to be disclosed by the recipient for delivering the money. These days, the prevailing trend is, mobile number of the receiver is given to the hawala operator, whose persons will contact the mobile holder, verify the codeword/password and then deliver the amounts. Thus, this system relies solely on mutual trust only. This system avoids scrutiny, documentation and encourages tax evasion and it is a tool for transfer of black money. This aspect makes it a popular mode of money transfer system. Since it is considered to be fast, reliable and cheap it is used as safe tool for money laundering.

1.1.3

Hawala transactions are illegal in India and are prohibited under Section 3 of the Foreign Exchange Management Act, 2000 and also under the Prevention of Money Laundering Act, 2002 as these transactions may involve transfer of criminal proceeds also. However, such transactions still continue to be prevalent in India. The reason is due to the subtle encouragement given to such transactions by the corrupt politicians', public servants, business men and black marketers for transferring money within the country and overseas. Further, organized crime cartels and illegal immigrants in India who do not have access to the formal banking systems will use this system for transfer of funds. As Hawala transactions do not require any proof of identity or documentation and are based on trust, it is considered as one of the ideal, safe and attractive methods of concealing the source of illegally obtained money and thus attained popularity. However, there is a decrease noticed in these transactions with the introduction of digitalization process in the financial institutions. As a result, it is observed that there is a shift towards abuse of digitalization process and financial institutions are being used for facilitation of money laundering processes by the criminals.

2. Types of Money Laundering through abuse of Digitalization process:

2.1 Use of Money Mules to Launder Criminal Proceeds:

One of the significant modus operandi adopted in money laundering scheme is the use of money mules. Money mules are people who are used to transfer ***"proceeds of crime"*** , either by laundering stolen money or physically transporting goods. Money mules may be willing participants and are often recruited by criminals through job advertisements. Money mule recruiters are also known as ***"Mule Herders"*** . Money mules may be knowingly complicit in the laundering of funds or work unwittingly or negligently on behalf of a Criminal Gang. Money

laundering network frequently recruit money mules from different sections of the society. A substantial amount of money mule transactions are linked to **cybercrimes, such as phishing, malware attacks, credit card fraud, business e-mail compromise,**
various types other scams like **lottery and employment scams**
. Some of the money mules may be unaware that they are being used to facilitate criminal activity. Unwilling unwitting mules are used by the Criminal Gangs to cash counterfeit cheques and money orders or purchase merchandise using stolen credit card number or personal identification information like AADHAAR CARD etc. Until recently, money mules were viewed as low level offenders transferring small amounts of cash. However, organized and sophisticated money mules have evolved innovative money laundering mechanisms. These money mules networks are often controlled by a hierarchical structure which is well resourced and highly effective in laundering funds. The money mules generally work in association with the Criminal Gangs. Money mule networks are often seen to open numerous individual bank accounts locally as well as in global financial centers and facilitate movement of criminal proceeds. Bank accounts opened by the mules serve as the initial layering stage in the laundering process. This indicates that criminals still find the combination of money mule accounts, cash withdrawals and wire transfers to be an effective way to layer proceeds of crime.

2.1.1 To illustrate the modus operandi of the money mules, the following example is given:

A person by name Mr. X was recruited by a criminal gang to receive money into his bank accounts. He was promised commission of up to Rs. 5000/- for each such transaction. Accordingly, Mr. X received criminal proceeds derived or obtained from a fraud committed outside India into his bank accounts. Most of the 'criminal proceeds' were either transferred out or withdrawn by him immediately on receipt, upon the instructions of the Criminal Gang.

2.1.2
Not only did Mr. X may serve as a recipient of illicit proceeds, he may also recruit some more money mules. The control of the mules' bank accounts allowed him to obscure the locations of the illicit proceeds through layering, and enabled him to evade detection of the 'criminal proceeds' as the funds were spread out over multiple accounts. Through this network, Mr. X and his money mule network receives 'proceeds of crime' and transfers the same into multiple accounts and or withdraws them within a couple of days. By doing so, Mr. X and his network had succeeded in obscuring the source of these illicit funds and aided in projecting these 'proceeds of crime' as untainted. Mr. X by commission of the above criminal acts, relating to scheduled offence is guilty of the offence of money laundering under Section 3 of the PMLA, 2002 and liable for punishment under Section 4 of the Act.

3. Use of Cash Deposit Machines at ATM's

Anyone can act as a professional launderer for an unknown Money Laundering Network. Mr. 'Y' opened bank accounts which were used to deposit crores of rupees of 'proceeds of crime' in cash. Multiple deposits each one of Rs. 49000/- were paid into these bank accounts per day using cash deposit machines in the ATM facilities. The cash deposit machine in the ATM is a facility to deposit, cash in his own account or to a third-party account, of course, a sum less than Rs. 49000/-. This facility will allow cash to be deposited at a quicker pace, at more locations and is often without coming into contact with staff. Once the cash deposited or paid into the bank accounts, money can be transferred to third-party bank accounts using bank procedure. Mr. 'Y' will be paid commission or incentive for moving the cash.

4. Avalanche Network [2]

4.1 Avalanche is an example of a criminal infrastructure dedicated for facilitating privacy invasions and financial crimes on a global scale. Avalanche was a hosting platform composed of a worldwide network of servers that was controlled via a highly organized central system. This cyber network hosted more than two dozen of the world's most pernicious types of malware and several large scale Money Laundering campaigns.

4.2 The Avalanche network, in operation since at least 2010, was estimated to serve clients operating as many as 500,000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of USD worldwide.

4.3
The Avalanche network offered cybercriminals a secure infrastructure, designed to thwart detection by Law enforcement and cyber security experts. Online banking passwords and other sensitive information stolen from victims' malware-infected computers, was redirected through the intricate network of Avalanche servers and ultimately to back-end servers controlled by the cybercriminals. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive, dark web criminal forums.

4.4 The types of malware and money mule schemes operating over the Avalanche network may vary. Ransom ware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of crypto- currency) to the cybercriminal. Other

malware, such as GozNym, was designed to steal sensitive online banking credentials from victims in order to use those credentials to initiate fraudulent wire transfers from the victims' bank accounts.

4.5
The Money Laundering schemes operating over Avalanche involved highly organised individuals, who controlled server networks and money mules, which were a crucial part of the criminal network. In some cases, the leaders would use a network of individuals to open bank accounts in major global financial hubs to facilitate wire transfers. The mules purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

5. Laundering Proceeds from Dark Web Drug Stores [3]

Investigators found that sale of drugs is taking place via the Dark Web. It offered payment option to the customers to pay and transfer funds for their order either by an indicated e-wallet, held in fiat currency, or to a Bitcoin address.

5.1 The financial scheme for the drug stores was arranged and managed by a financier and his network. The Money Laundering network was responsible solely for moving funds and had no links to drug trafficking. Numerous e-wallets and debit cards were registered in the names of the front men. This modus operandi usually involved students who were issued e-wallets and credit cards and then sold them to members of the Money Laundering network. They are unaware of the criminal purpose of their further usage.

5.2
The investigators observed that, to simplify the Money Laundering process, the network's IT specialists developed a 'transit panel' that had a user-friendly interface and was accessible via the TOR browser. The transit panel automatically switched between e-wallets that were used for drug payments. Digital money was automatically moved through a complex chain of different e-wallets. Money from e-wallets was then transferred to debit cards and withdrawn in cash via ATMs. Withdrawals via ATMs were conducted by "cash coordinators" who had multiple debit cards at hand. Afterwards, cash was handed over to interested parties. In order to increase the complexity, proceeds were re-deposited on a new set of debit cards and transferred to the Criminal Gangs.

6. Trade-Based Money Laundering Scheme

6.1 Trade Based Money Laundering (TBML) is a process of disguising the 'proceeds of crime' and moving value through the use of trade transactions in an attempt to legitimize their illicit origin [4]
. The various modus operandi employed by the Money Launderers involve the following:

- Purchase of high value goods using 'proceeds of crime', ship the goods and re-sale of goods in the destination country abroad.

- The transfer of funds purported to be related to trade, or for the purchase of goods that were never shipped or received. This is also known as 'Phantom Shipments'.

- Under invoicing of import goods

- Using the proceeds of crime to purchase goods for legitimate re-sale with the payment for goods made to drug traffickers by legitimate businessman.

6.1.1
By using the Trade Based Money Laundering modus operandi, the money launderers will break the link between the predicate offence and the related money laundering. This will make the job of investigator difficult to link the 'proceeds of crime' with the crime/criminal.

6.2 TBML through shell companies:

Trade Based Money Laundering (TBML), was resorted to by a group of criminals where two of the group's central figures hired some nominees to establish several shell companies. The shell companies were opened using names across a diverse number of industries like plastics, construction, electronics etc.

6.2.1
The laundering network included legitimate businesses, operating in the financial and construction sectors, as well as a financial company,

which was complicit in laundering the funds. The money launderer provided his accomplice at the financial company with large bags of cash, which is nothing but 'proceeds of crime' derived or obtained by commission of a drug related offence which was deposited into business accounts in the name of shell companies. The shell companies used to issue cheques in the name of those entities requiring legal amounts, the so-called white amount under the guise of loan on receipt of pre-agreed commission. This modus operandi is continued until the accounts were closed by the financial institution that held the shell company's accounts, due to a high volume of suspicious transactions.

6.3 Some of the funds may be transferred back to the drug traffickers residing abroad and to the companies controlled by the traffickers. This money will be used for purchase of goods and the purchased goods were then shipped to other foreign countries for sale. Once the purchased goods arrive at the destination country, they were sold, and the proceeds of the sale (in the destination country's currency) were then transferred to the drug trafficking or Money Laundering organization to provide the criminals with "clean" funds, for being again laundered through TBML.

In view of the above, it can be seen that there is an appreciable reduction in the prevalence of Hawala transactions. However, there is an increased abuse of digitalization process and the financial institutions are being used for facilitation of money laundering through opening of multiple accounts by the money mules and depositing and transfer of funds in small denominations /fragmented amounts through shell companies. Besides the above, sending criminal money abroad though shell companies as purchase value of the goods and the sale of purchased goods in the destination country and being proceeds re-transferred to drug traffickers to provide the criminals 'clean money' is often noticed in Trade Based Money Laundering offences.

[The author is working as Additional Commissioner (AR), CESTAT, Hyderabad and the views expressed are strictly personal.]

Editor: Also read Metamorphosis of Money Laundering Techniques - Crypto Currency and Money Laundering Â

1See Lisa (Carroll)
"Alternative Remittance Systems. Distinguishing Sub-Systems of Ethnic Money Laundering in Interpol Member Countries on the Asian Continent", https://www.emcdda.europa.eu/.

2https://www.fatf-gafi.org

3 http://www.fatf.org

4 FATF-2006