पर्यवेक्षण विभाग / Department of Supervision
केवाईसी एएमएल समूह / KYC AML Group
केन्द्रीय कार्यालय / Central Office
मुंबई / Mumbai

Confidential

Advisory **Dated: August 10, 2022**

Frauds / Cybercrimes through investment / part time job / ponzi scheme scams

Of late, we are witnessing the incidence of a number of cybercrimes wherein the criminals and fraudsters are resorting to different kinds of modus operandi for perpetrating cybercrimes routed through the banking channels and payment gateways. RBI, time and again, disseminates information about the frauds/cybercrimes and issue Advisories to the Regulated Entities (REs) which *inter alia* include the course of actions to be followed by the REs. In this regard, we further advise the banks regarding such frauds and cybercrimes which have come to our notice in the recent past.

2. Some of the **modus operandi** followed by the fraudsters and criminals through investment / part time job / ponzi schemes, wherein the transactions are routed through the banking channels are given hereunder:
   (a) Victims are lured through part-time job offers and other advertisements on Internet and/or messaging platforms, etc., and are promised high commissions or high returns such as doubling of money in short span of time. The advertisements / SMS messages usually contain a link, which directly prompts for a chat. Further, mobile applications, bulk SMS messages, SIM-box-based Virtual Private Network (VPNs), phishing websites, cloud services, virtual accounts in banks, Application Programming Interfaces (APIs), etc., are used to carry out financial frauds.
   (b) Keywords such as "Earn Online", "Part Time Job", etc., are used by fraudsters and criminals to match their advertisements with the terms people are searching

for. Further, such advertisements are mostly displayed from 10 AM to 7 PM, which is usually the peak time for internet use by Indian public.

Majority of websites used by fraudsters have domains - 'xyz' and 'wixsite'. Most of these sites either redirect to a messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.

(c) Multiple Indian numbers were used for communication with victims. Upon analysis, it was found that mobile number holder was not aware about messaging platform being operated in his/her name. In some cases, the mobile number holder knowingly shares OTP in return for some money from the fraudsters.

(d) The fraudster sends an investment link over chat. Each person has a referral code. Fraudster generally communicates in English. Google Translate is also used to communicate with the victims.

(e) A screenshot needs to be sent to the person over the messaging platform to activate the account. Once the account is activated, a task is given to the user to gain confidence of the person. Mandatory condition to do a task is to load money through Payment Gateways which are not authorized to operate in India. All payments are made through UPI. Some of the UPI addresses belong to companies registered with . A call centre is usually used to interact with the victim for communication regarding tasks. For instance, on failure to load funds on investment website, the call centre executive initiates a call.

(f) Once the task is completed, the victim is asked to withdraw the money. Money is withdrawn through various Payment Aggregators.

(g) On getting the first refund, the victim is now lured to do more tasks which involve loading of more money. The process continues and once a big amount is loaded by the victim, the person (fraudster) stops responding over chat.

(h) UPI details are updated daily on the fraudulent websites. Investment websites keep changing. Source code remains same but domain changes.

(i) Bank accounts opened by money mules using real / fake identification are used to receive stolen funds from compromised bank accounts, through sharing of OTPs, etc. Rented accounts are sourced by agents and account owners

(money mules) are given fixed rent or commission or lumpsum amount for the account.

(j) Layering of transactions is carried out by account to account transfers. Bulk payments / APIs are also used for this.

(k) From the intermediate account, money is diverted to multiple sources/assets like crypto currencies, bullion, payout accounts (for gaining confidence and hiding laundering), foreign money transfer, person-to-person transfer, etc.

(l) Instances have been observed where Shell Companies with dummy directors, rented companies with MCA registration certificates, fintech companies, payment gateways, SMS aggregators are reported to be involved in carrying out such financial frauds, mostly using UPI as payment mode. Main objective of opening Shell Companies is to create a current account or a fintech company for accepting or paying out proceeds of frauds. Most of these Shell Companies appear to be Technology Companies created with 'Technology Private Limited' name and mostly registered with

(m) UPI addresses are used to create layering behind Payment Aggregators thereby, facilitating end of day settlement.

(n) Aggregator on aggregator concept is used by these players (fraudsters) in order to conceal their identities. The merchants onboarded on the fintech players (Eg. ABC company onboarded on Payment Aggregator) are frauds. The network of fraudsters start creating Payment Aggregator business in collaboration with banks directly or with other fintech companies. The fraudsters would be sitting behind the payment aggregator as sub-aggregator or directly as a merchant. The money collected by the fraudsters, as sub-aggregator and/or as merchant, is remitted to the Payment Aggregator wherefrom the API(app) based payouts take place. After the aggregator network is set up, the accounts are operated for making the payouts by the fraudsters based outside India.

(o) Chartered Accountants, foreign nationals (from Cambodia, China, Dubai, Nepal, Philippines, etc.), payment aggregators, points of sale terminals for SIM cards, etc., are also reported to be involved in such frauds.

(p) Gold, crypto currencies, international money transfers are observed by Law Enforcement Agencies (LEAs) to be the usual termination points of the fraud trails.

3. Weaknesses in Customer Due Diligence (CDD) and transaction monitoring

The following weaknesses have been observed on the part of the banks, customers and other concerned entities:

(a) Lack of adequate CDD and verification of credentials for customer onboarding;

(b) Lack of mechanism to identify the potential 'money mule' customers and inadequate transaction monitoring mechanism for such accounts;

(c) Inadequate due diligence for opening accounts of companies which are actually 'Shell Companies';

(d) Inefficient and inadequate AML monitoring of accounts of purported fintech companies and payment aggregators for suspicious transactions;

(e) Lack of adequate awareness among the customers regarding the vulnerabilities of using digital channels and social media;

(f) Lack of on-going employee training programmes for updating them with the latest KYC / AML concerns.

4. Identification and Monitoring of Money Mule Accounts

In order to prevent the misuse of the banking system by the fraudsters and the money launderers through the accounts of money mules, *in general*, and to prevent and protect the gullible public from falling prey to such fraudsters and money launderers, *in particular*, the banks are advised to put in place a comprehensive mechanism, duly approved by the Board / Audit Committee of the Board, to identify and monitor the suspected money mule accounts. The mechanism to be put in place by the bank should *inter-alia* include / envisage the following:

(a) The accounts of natural persons (1) having very low balance (say a few hundred rupees) and not operated for more than a year, **or** (2) having been opened as small accounts, **and** (3) receiving multiple credits of small amounts in quick succession in a very short span of time followed by immediate withdrawals (cash or transfer, single or multiple), should be flagged as suspected money mule accounts;

(b) Any such account, which has been flagged as suspected money mule account, should immediately be subjected to Enhanced Due Diligence (EDD) and enhanced monitoring without any tip-off to the customer. The transactions routed

through these identified / suspected money mule accounts should be examined for suspicious transaction reporting to FIU-IND;

(c) The banks may fix separate turn-around time for scenarios involving money mules for processing of AML alerts; and

(d) The system for identification of an account as money mule should be completed in a time bound manner within 6 months from the date of this Advisory.

5. Course of actions:

Keeping in view the large number of frauds perpetrated through the aforesaid modus operandi, banks are required to take actions, on priority basis and in a time bound manner, which *inter-alia* should include the following:

(a) Give special emphasis on strengthening the KYC / AML framework put in place like customer due diligence (including enhanced CDD, wherever required), name screening, customer risk profiling, real-time transaction monitoring system, AML alerts and examination, etc., for accounts used as money mules, accounts opened by Shell Companies, accounts of fintech players etc.; ensure effective monitoring of Payouts in case of accounts of fintech players and reporting of suspicious transactions to FIU on the same. Further, sufficient controls may be deployed for UPI transactions with enhanced monitoring on the suspicious UPI IDs mentioned in regular LEA references and various other sources.

(b) Ensure that sufficient control measures are in place to monitor the transactions of digital delivery channels and reporting the suspicious transactions to FIU, even if the outsourced service providers are involved in such delivery.

(c) Continue to create awareness among the customers for NOT sharing the OTP, login credentials and other banking security information and NOT to send money as initial deposit, commission or transfer fee to anyone claiming to provide huge, usually unrealistic, returns from known or unknown organisations/persons;

(d) Place the modus operandi, and the precautionary measures to be taken by the customers, on the website for wider circulation and awareness among the members of public.

(e) **Note:** While circulating the precautionary measures and other information from this Advisory, care should be taken that specifics related to name of the entities

/ professions / jurisdictions mentioned in this Advisory are not disclosed to the customers or in the public domain in any manner;

(f) Bring the modus operandi and the control measures laid down by the bank to the notice of all the controlling offices / branches, so that recurrence of such modus operandi can be arrested / minimized;

(g) Consider the above factors, while undertaking the next round of ML / TF internal risk assessment, as required in terms of Para 5A of the RBI Master Direction on KYC dated February 25, 2016, as amended from time to time;

(h) Design KYC / AML training courses for the staff with the latest KYC / AML concerns flagged by the competent authorities and as identified by the banks;

(i) Share the modus operandi with the Internal Audit Department of the bank for factoring the same in their risk assessment during the risk based annual internal audit programme.