Press Release

02.09.2024

Directorate of Enforcement (ED) has arrested 03 persons namely Shashi Kumar M (aged 25 years), Sachin M (aged 26 years) and Kiran S K (aged 25 years) on 15.08.2024 and 01 person namely Charan Raj C (aged 26 Years) on 21.08.2024 in Bengaluru in a case related to Cyber Investment Scams in which innocent persons are being cheated and defrauded of their hard-earned money by inducing them to invest in stock markets through fake and fraudulent Apps. All the four accused were involved in incorporation of companies and opening of bank accounts, through which proceeds of crime generated from cyber scam were laundered. Hon'ble Special Court, Bengaluru had remanded the ED custody of these 04 accused persons for 7 days each.

So far, 13 searches have been conducted u/s 17 of PMLA, 2002 at various premises which led to seizure of various incriminating material including mobile phones and other digital devices. ED investigation under PMLA, 2002 has, so far, traced Proceeds of Crime of more that **Rs 25 Crore** generated from this Investment Cyber scam.

Brief facts of the predicate offence

PMLA Investigation into the case is based on several FIRs registered by various state police all over the country. Summary of the contents mentioned in some of these FIRs are as under: -

a) **Faridabad FIR**: In this FIR, a victim in Faridabad was cheated of **Rs 7.59** Crore by the scamsters by inducing her to invest in stocks through fake Apps. The victim had clicked on a Share Market investment link while browsing Facebook, after which she was added to a WhatsApp group named **ICICI IR Team (57)**. She observed the Whatsapp group for a few months, and noted that many members in the WhatsApp group (which were planted by scamsters for posting fake messages) were reporting high returns on their investments. She was not aware that these persons were actually planted by the scamsters for posting fake messages. After giving her willingness, she was added to another WhatsApp group named **C6RAM Investment Academy**.

Thereafter, victim was instructed by the WhatsApp group admin to install an app named **IC ORGAN MAX** and to open an account on the App using her mobile number. Further, the WhatsApp Group Admin asked victim to get details of the bank account (in which the funds need to be transferred for getting the same added in the app) from their customer care number available on the App. Victim transferred Rs. 61 Lakh in the bank account number provided by Customer care of the App **IC ORGAN MAX.**

Thereafter, victim was asked to install another app named **Techstars.shop** using a registration link provided by scamster. She opened an account on this app also using her mobile number and transferred money to various accounts. A total of **Rs. 7.59 Crore** was defrauded from her under false promises of high returns, resulting in FIR 040/2024 dated March 29, 2024, under sections 420 and 120-B of IPC, 1860.

b) **Noida FIR**: Similarly, another businessman in Noida was cheated of Rs 9.09 Crore by the scamsters who had added him to a Whatsapp group named **GFSL Securities official Stock C 80**. By adopting similar modus as described above, he was induced to download an App and made to transfer **Rs. 9.09 Crore** to various bank accounts provided by customer care of the App.

c) **Bathinda FIR**: By adopting similar modus operandi, a Doctor in Bhatinda, Punjab was defrauded of **Rs. 5.93 Crore** by inducing him to download a fake App namely **GFSL Securities** when he was browsing Facebook and transfer fund in the name of investment in stock market.

Similar modus operandi has been adopted by fraudsters in various other FIRs to cheat innocent persons by luring them to transfer their hard-earned money on the pretext of investment in high return yielding financial products through fraudulent Apps.

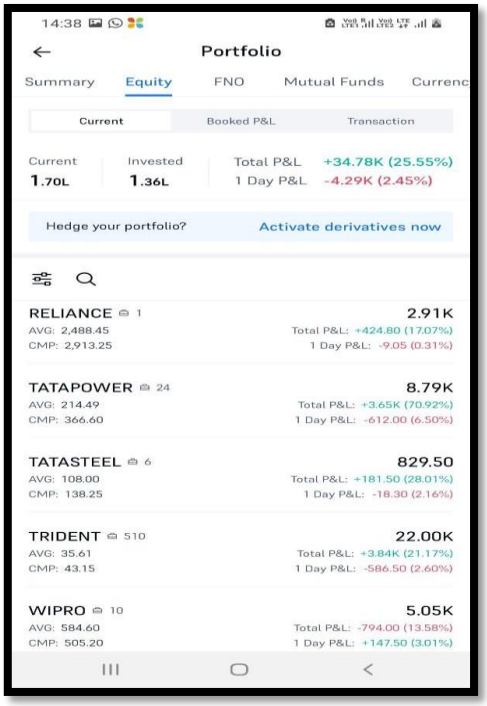
Modus Operandi of Investment Cyberfraud

The investigation conducted under the PMLA, 2002 has revealed that victims of the aforementioned cyber scams are being cheated through fraudulent stock market investment options in following manner: -

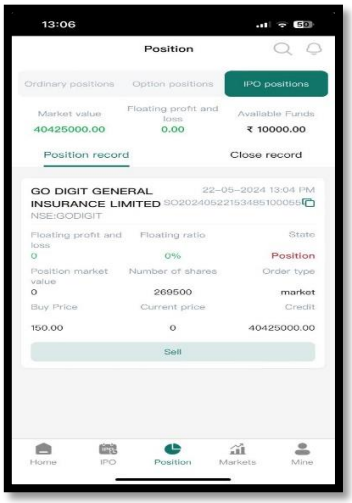
a) **Luring Victims**: The first step of scam involves luring the victims via various social media platforms including Facebook, Instagram, WhatsApp, and Telegram by giving false promises of high return on their investment, allotment of IPOs through special quota, etc.

b) **Fake Groups:** Once the victims seem interested, these scamsters then add these victims to WhatsApp/Telegram Groups, which also have fake members planted by these scamsters in these groups for sharing fake and fabricated success stories in these WhatsApp group. These WhatsApp groups have names similar to well-known apps/financial institutions e.g. ICICI Securities, GFSL Securities, SMG Global Securities, Blackrock Capital, JP Morgan to create an impression that these groups are genuine.

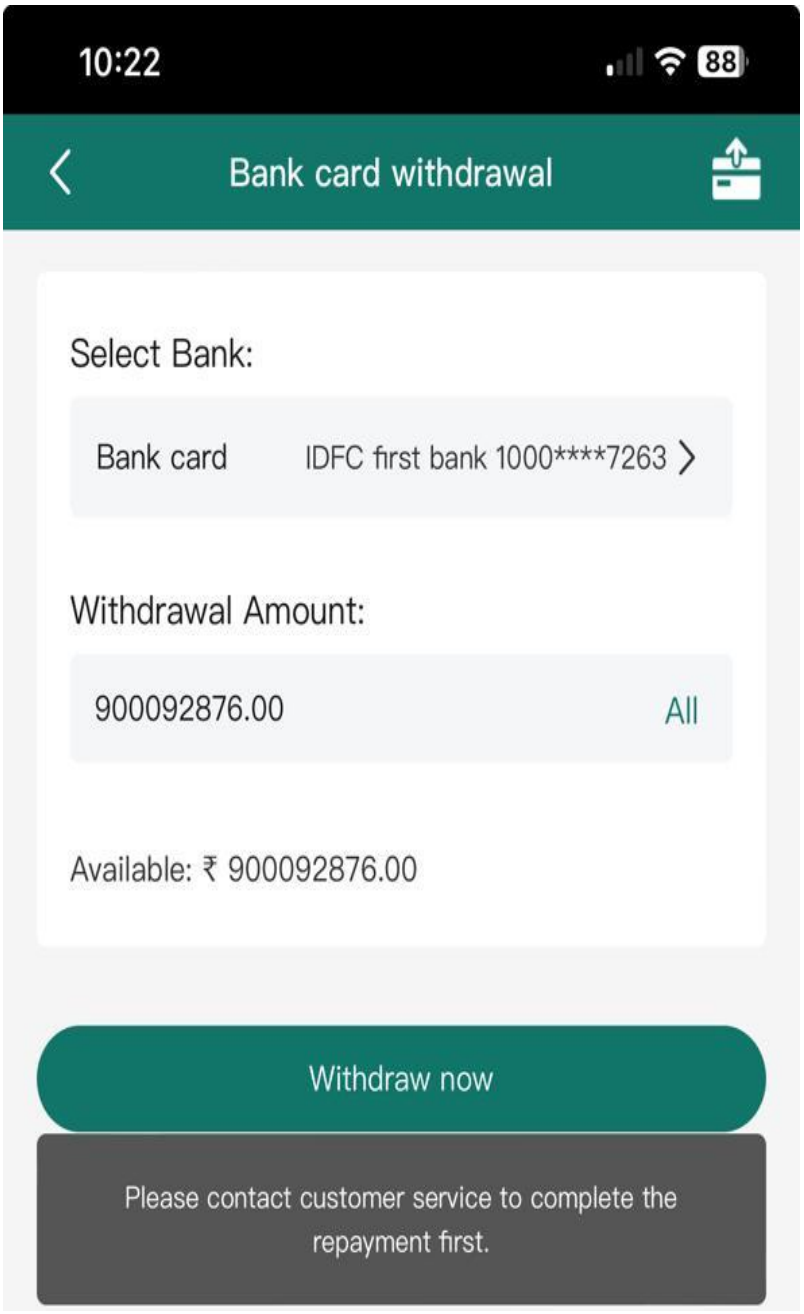
c) **Fake Apps**: Once the victims are convinced about the genuineness of the WhatsApp/Telegram Groups and the fake success stories planted by members, scamsters then ask these victims to install fraudulent apps for the purpose of investments. For the purpose of installing the Apps, Scamsters share the links or apk file over WhatsApp to the victim. The names of various stocks, futures, option, forex etc. shown in these apps are the same as that of well-known companies (e.g. Reliance, Tata power) to create an impression that the Apps are genuine. Screen shot of one of such fake app is as under:-



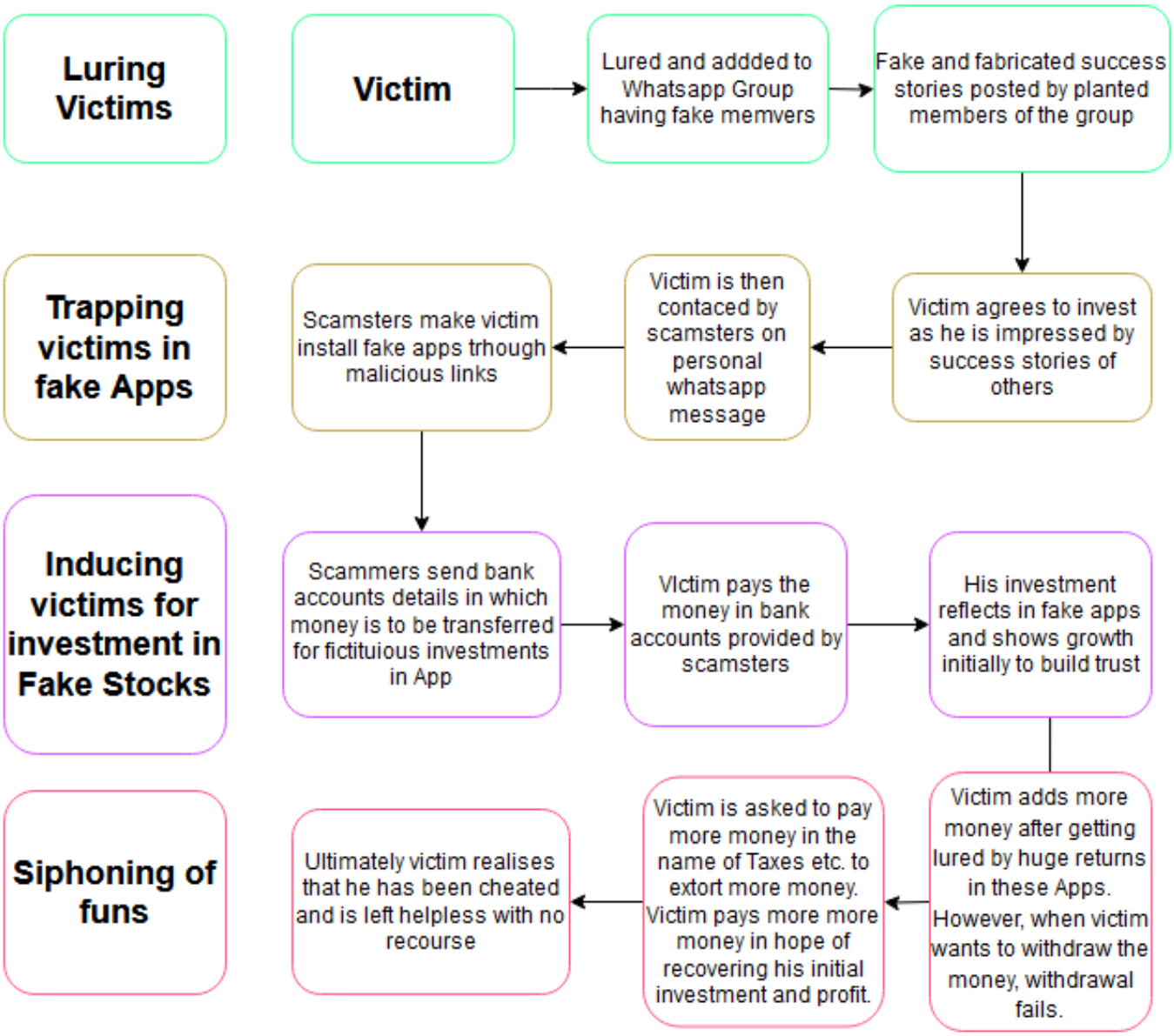
d) **Fake Investments**: Thereafter these scamsters induce the victims to invest in various fake IPO stocks, fake Stocks, etc. and make them transfer their hard-earned money to the bank accounts of shell companies created for the specific purpose of collection of cybercrime proceeds. Thus, these victims are duped of their hard-earned money. A screenshot of the fake app showing fake IPO stock (having same name as the real IPO) wherein the victim had invested is as under: -



e) **Siphoning the Funds:** To build further trust, the victim might initially get good returns on their investment as shown in the dashboard of App, which gives them confidence and encourages them to invest more amounts. These returns are entirely fictitious and do not exist in reality. They are just numbers shown on these fake apps. As the victim invests more funds, they eventually realize that they are unable to withdraw their funds. When the victims try to withdraw their money from these apps, the scammer asks the victims to pay statutory taxes, brokerage fees, etc. which are nothing but ways to extract even more money from the victims. Once the scammer believes that they have extracted as much money as possible, they cut off all communication and disappear, leaving the victim helpless and with no recourse. A screenshot of the app showing the message '*Please contact customer care to complete the repayment first'* when the victim tried to withdraw his money is as under:-


10:22
88
Bank card withdrawal
Select Bank:
Bank card
IDFC first bank 1000****7263
Withdrawal Amount:
900092876.00
All
Available: ₹ 900092876.00
Withdraw now
Please contact customer service to complete the repayment first.

f) The whole modus operandi is depicted in diagram below:



Cyberscam: Behind the scenes

a) **Arrangement of SIM Cards**

Scammers contact various individuals within India via Telegram groups to acquire hundreds of SIM cards illegally. There are various Telegram groups where black marketers provide SIM cards.

A screenshot of a telegram group is as below:

After activation, these SIM cards are shipped abroad. These SIMs are either linked with the bank accounts of multiple shell companies or used to create and run the WhatsApp accounts for the purpose of defrauding victims.

b) **Creation of Shell Companies**:

Scammers incorporate hundreds of shell companies specifically for acquiring and siphoning off Proceeds of Crime generated from these Cyberscams. They use the addresses of coworking spaces to provide a physical/virtual address for the incorporation of these shell companies. Further, it is revealed that during the filing of Form INC-20A (required to be filed on MCA portal for commencement of business by company), scammers have submitted forged bank statements as proof of share subscription by shareholders. Investigation has further revealed that the scammers operate through a network of mule bank accounts which are rented through channels such as Telegram. Investigation has revealed that the Proceeds of crime is finally converted into crypto currency and siphoned off abroad to avoid detection and recovery.

c) **Money Movement through Shell Companies**: Funds are moved from the victim's account through several intermediary accounts including Mule Accounts (taken on rent by scamsters) for layering the PoC. This involves numerous transactions between accounts to create a convoluted web that conceals the original source of the funds. Small transaction amounts (less than Rs. 5 lakhs) are used to avoid triggering alerts for suspicious activity. The illicit funds are routed through these shell companies.

d) **Cryptocurrency**: A key finding of the investigation is that the proceeds of these fraudulent activities were mostly converted into cryptocurrency. This conversion was a deliberate strategy employed by the accused to further obscure the origins of the illicit funds and to facilitate their transfer out of India. By converting the proceeds into cryptocurrency and transferring them abroad, the perpetrators aimed to avoid detection, tracing, and recovery by law enforcement agencies.

e) Human Trafficking and the use of Foreign Jurisdiction:

The Golden Triangle, located at the intersection of Thailand, Laos, and Myanmar, has long been known for illicit activities, including drug trafficking and human trafficking. Indian citizens are lured on the pretext of job offers and trafficked to this Golden Triangle and are being exploited in cyber fraud operations including this Cyber Investment Scam. Criminal networks force victims to work in call centers or engage in online scams, under harsh and coercive conditions.

Further investigation is under progress.