



Central Depository Services (India) Limited

Convenient ⊕ Dependable ⊕ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/OPS/DP/POLCY/2024/404

July 19, 2024

REPORT OF INDIAN CYBER CRIME COORDINATION CENTRE WITH RESPECT TO ABUSE OF 'SMS HEADERS' IN TRANSNATIONAL 'STOCK MARKET INVESTMENT FRAUD'

DPs are advised to refer to the SEBI report dated April 18, 2024 of Indian Cyber Crime Coordination Centre titled Abuse of 'SMS Headers' in Transnational 'Stock Market Investment Fraud' (copy of the report attached herewith).

In this regard, DPs are advised to take necessary measures, as mentioned in the report, including the following:

1. Measures to prevent misuse of their SMS headers, entity and template ID by telemarketer or through DLT platform.
2. Measures to follow directions dated February 16, 2023* issued by TRAI (Ref. CDSL Circular No.: CDSL/OPS/DP/POLCY/2023/200 dated March 29, 2023) to curb misuse of Headers and Content Templates. Also review all Headers and Content Templates and surrender/close unused Header and Template.
3. Measures for prompt reporting of any impersonation of their identity, trademark, logo etc. by any fraudster on National Cybercrime Reporting Portal.

DPs are advised to take note of the same and ensure compliance.

Queries regarding this communiqué may be addressed to: CDSL – Helpdesk Emails may be sent to: dprtasupport@cdslindia.com and connect through our IVR Number 022-62343333 .

For and on behalf of
Central Depository Services (India) Limited

sd/-

Akhil Wadhavkar
Chief Information Security Officer



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Indian
Cyber
Crime
Coordination
Centre

**NATIONAL CYBERCRIME THREAT ANALYTICS UNIT
TAU – 115 | Telecom Intelligence Report**

**Abuse of ‘SMS Headers’ in Transnational
‘Stock Market Investment Fraud’**

Prepared By
Indian Cyber Crime Coordination Centre (I4C)
Ministry of Home Affairs
New Delhi

18th April 2024



@cyberdost4c



@CyberDost4c



@cyberdost4c



@cyberdost



@cyberdost4c



@cyberdost.4c



@cyberdost4c



@cyberdost



@cyberdost

Table of Contents

1. Introduction.....	3
2. Executive Summary.....	3
3. Observations	4
4. Recommendations.....	5
5. Details of SMS Headers being Misused.....	6
6. Screenshots of SMSes	7
7. Confirmation from Entities.....	9

1. Introduction

The Ministry of Home Affairs, Government of India has established the **Indian Cyber Crime Coordination Centre (I4C)** to provide a framework and eco-system for Law Enforcement Agencies (LEAs) to deal with cybercrime in a comprehensive and coordinated manner. The **National Cybercrime Threat Analytics Unit (NCTAU)** is one of the vertical of I4C which is instrumental in issuing alerts, advisories, and carrying out analysis of cyber threats and sharing the reports with various Ministries / Department, and other stakeholders for the prevention of cybercrime in the country.

2. Executive Summary

National Cybercrime Threat Analytics Unit has observed a sharp rise in a new pattern of transnational cyber enabled financial fraud. During analysis of National Cybercrime Reporting Portal complaints and inputs from State Police, a new pattern of transnational investment scam is observed where the cyber criminals are impersonating stockbrokers, financial advisors, or company executives of capital investment companies majorly through fake mobile apps, websites, and WhatsApp / Telegram. Fraud WhatsApp groups are learnt to be operated from Cambodia / Hong Kong.

At the early stage, these apps were learnt to be circulated through Google Playstore, Apple App store and via web links that are sponsored majorly through Instagram and Facebook Advertisements targeting users with 'interest' in 'Stock Market'.

Recently, it has been observed that the cybercriminals have started abusing A2P SMS by sending bulk SMSes to the potential victims with

luring messages and a link which redirected to a WhatsApp group where further crime takes place.

3. Observations

- It is observed that there is potential takeover / misuse of SMS Header, Entity and Template ID from either Telemarketer end or through DLT platform.
- These Identifiers are being used to send SMSes by cyber fraudsters without consent / knowledge of Entity / Header Owner which is a serious cause of concern as victims believe the SMS is coming from genuine entity and proceeds with the messages.
- Fraud SMS containing link to join WhatsApp group are being sent through **V-CON Mobile & Infra Private Ltd. (VM IPL)** and **Bharti Airtel**.
- NCTAU has confirmed from some of the entities that they have not sent the SMS and header / template has been mis-used.
- It is also found that the SMS Header Entity as well as template are totally different, and the SMS being sent relating to Stock Market through these headers.
- A report on misuse of SMS Headers related to similar threat actor / modus operandi had also shared with TRAI vide report no. **TAU-042**.

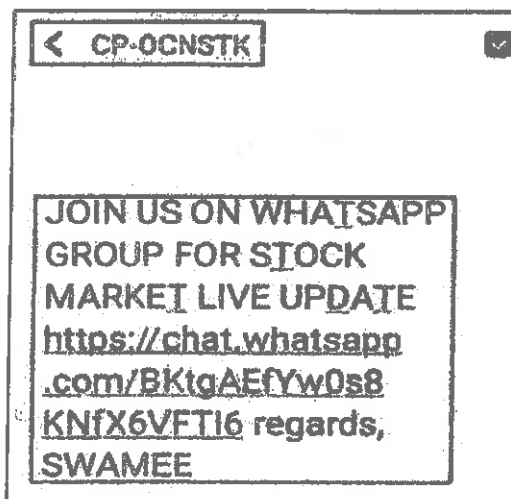
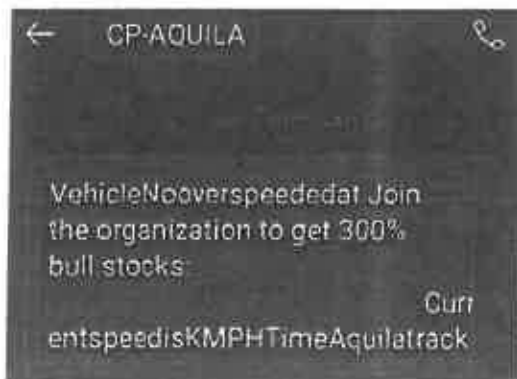
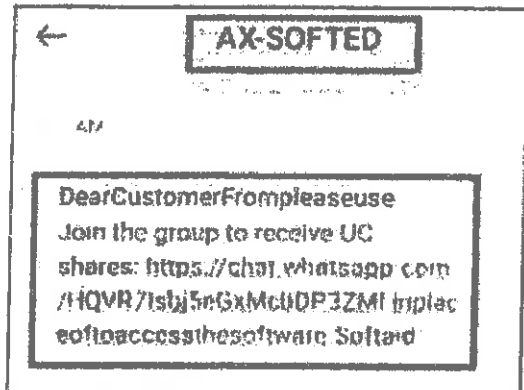
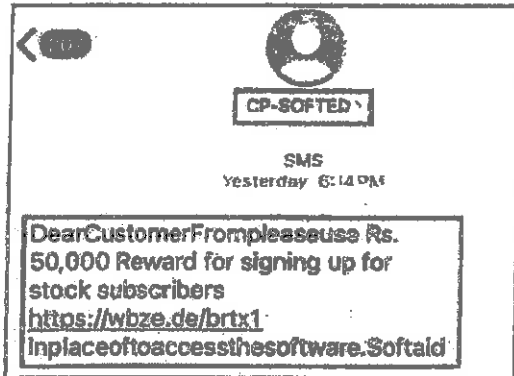
4. Recommendations

- Identify the root cause of the misuse / hacking of Entity ID, Header ID and Template ID.
- Identify the Tele-marketer involved in sending the messages shared in the report.
- Gauge the scale of abuse and number of SMS sent along with the source of phone numbers used by TM to send SMS.
- Telecom operators may implement AI based detection mechanism to detect WhatsApp group links and redirecting web links.
- Explore option to put additional authentication mechanism which will ask for re-authorization in case of Tele-Marketer change.


5. Details of SMS Headers being Misused.

Sr.No.	Prefix	Header	Principal Entity and Address	Purpose
1.	CP	SOFTED	SOFT AID COMPUTER 18/2, Ramdas Colony, M J College Rd JALGAON, Jalgaon, Maharashtra, 425001	Transactional/Service
2.	CP	RESHMT	Reshma Tourists Shop No 17, S.NO 124 1 A, Rajeev Gandhi Vanijya Sankeerna, Marpady Village, Mudbidri, Dakshina Kannada, Karnataka	Transactional/Service
3.	CP	AQUILA	Zellot Connected Services Private Limited 803/1, 803/A-1-3, 76th A Cross, West of Chord Road, 6th Block, Rajajinagar	Transactional/Service
4.	CP	OCNSTK	OCEAN STOCKS 606, Golden Traengal, Opp Stediam, Post Navjivan, Ahmedabad	Transactional/Service
5.	CP	ZIGMAZ	Meenakshi Ammal Educational Trust, No.81/82,Veerabathra Nagar,Medavakkam,Chennai, Kancheepuram, Tamil Nadu, 600100.	Transactional/Service
6.	CP	PSRDFM	PSR Dairy Farm 77/3 Near Rto Office, Peruvangur Village,Kallakurichi, Kallakkurichi, Tamil Nadu, 606213	Transactional/Service
7.	CP	TRAMCO	The Ramco Cements Limited, Ramamandiram, Rajapalayam, Rajapalayam, Tamil Nadu, 626117	Transactional/Service
8.	AX	DBSJNP	Smt dhanraji devi shri bhuleshwar singh inter college, kadipur, ramdayalganj, jaunpur, uttar pradesh, 222105.	Transactional/Service

6. Screenshots of SMSes



189



CP-ZIGMAZ


SMS
Today, 11:39 AM

Dearkindlyjointhemeetingreg Join the group to receive UC shares: <https://api.whatsapp.com/send?phone=919725337838>
zoomidpwdRegardsZIGMAMHSS



PSRDAIRYFARMDEIAMLtr Professional Stock Analysis Link: P/MLT/

210




AX-DBSJNP

SMS
Today, 1:52 PM

DearParentsAdmissionsareopenfor Professional Stock Analysis Link: chat.whatsapp.com/ISV4QvW4IG1AMk8ibUsf1A
toFROMDBSINTERCOLLEGE

189



CP-TRAMCO

SMS
Tuesday, 11:03 AM

CementdeapMTQdMtd Blackstone recommended fine stock, click to get it now!
<https://wa.me/919908788185>
RamcoCements

Tuesday, 12:08 PM

CementdeapMTQdMtd Professional Stock Analysis Link!<https://api.whatsapp.com/joinchat/CPs4uMlCedJndw>
RamcoCements

Tuesday, 12:08 PM

CementdeapMTQdMtd Blackstone recommended fine stock, click to get it now!
<https://wa.me/919908788185>
RamcoCements



7. Confirmation from Entities

Email Communication to Softed Computers

softaid computer April 15, 2024 1:04 AM

Good Morning,

As discussed over telephonically, please see the following SMSes being forwarded through your registered SMS Header with TRAI and requested to kindly confirm that whether these SMSes are being sent through your company or not.

 SMS Wednesday, 7:12 AM Dear Customer From please use Rs. 50,000 Reward for signing up for stock subscribers https://wbze.de/btrx1 inplaceoftoaccess the software. Softaid	 Dear Customer From please use Join the group to receive UC shares: https://chat.whatsapp.com/HQYB71abj5eGxMcbDPJZMI in placeoftoaccess the software. Softaid
---	---

Response from Softed Computers

Request for confirmation - reg 2 messages

From: softaid computer April 15, 2024 1:30 PM


Hi,

Dear sir,
After reviewing the messages forwarded to us, we can confirm that they were not sent by our company.

Regards,
Suresh Wankhede
www.softaidcomputers.com | softaid.computer@gmail.com

Email Communication to Zeliot

Request for confirmation - reg 2 messages

 From: akshay@zeliot.in April 15, 2024 12:44 PM

To: akshay@zeliot.in

Good Afternoon,

As discussed telephonically, please see the following SMS being forwarded through your registered SMS Header with TRAI and requested to kindly confirm that whether this SMSes are being sent through your company or not.

← 9794301614


VehicleNooverspassedat Join
the organization to get 300%
bull stocks.

Curr
entspeedsKMPIITimeAquilatrack

An early response in this regard will be highly appreciated.

Response from Zeliot

Request for confirmation - reg 2 messages

 From: akshay@zeliot.in April 15, 2024 5:10 PM

To: akshay@zeliot.in

Cc: sumeet@zeliot.in anup@zeliot.in

Hi

These SMSs are not being sent by us. We are not into this business case. This seems to be a case of hacking and on this suspect, we have blocked the this header through our gateway partner.

Kindly let me know if any additional action needs to be taken.
