

Shadow Banking in Your Pocket: Exposing Android App Used by Money Mules



Report

Intelligence Type

Adversary Intelligence

Threat actor Motivation

Financial

Industry

Banking & Finance

Region

India

White papers and reports can be downloaded from CloudSEK website by visiting <https://cloudsek.com/whitepapers-reports> or by mailing to info@cloudsek.com.

What are Money Mules ?

A money mule refers to an individual enlisted to receive and transfer funds acquired through fraudulent activities. This role is pivotal in the execution of various financial crimes, such as cyber fraud or money laundering. Importantly, the involvement of money mules introduces an additional layer of complexity, making it challenging for law enforcement to trace the origins of illicit transactions.

In October 2023, CloudSEK identified a critical loophole within India's banking infrastructure. This loophole was actively exploited by Chinese cybercriminals to orchestrate a large-scale money laundering scheme targeting Indian citizens. The scheme leveraged a network exceeding hundreds of thousands of compromised "money mule" accounts to funnel illicit funds through fraudulent payment channels, ultimately transferring them back to China.

Link to the Report: [Chinese Scammers Launder Money via Fraud Payment Gateways: A New Threat to India's Digital Payment Ecosystem](#)

CloudSEK's Threat Intelligence (TI) team continued its investigation and has uncovered a network of money mules, posing a significant risk to the Indian banking ecosystem. This report focuses on a malicious mobile application (APK) identified as a key tool for onboarding and managing these money mules. Through in-depth analysis, we reveal the functionalities of this APK and the vulnerabilities it exploits, shedding light on the inner workings of this criminal operation.

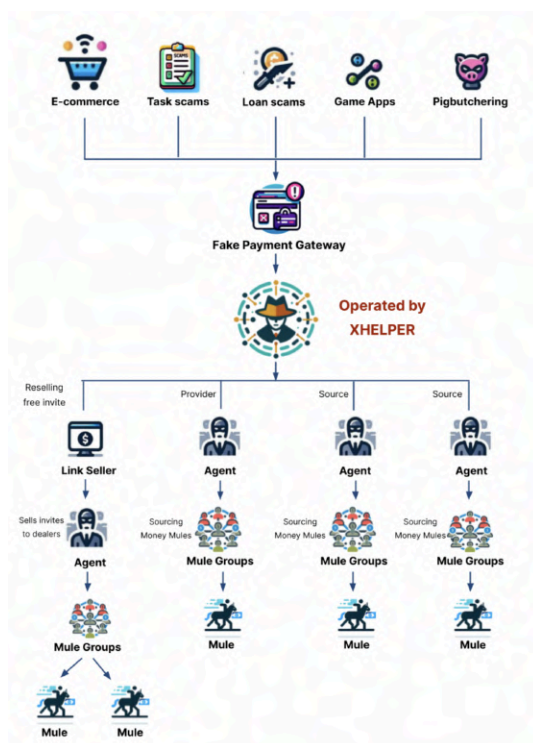


Image Showing Scam Operations Weaponizing Money Mules

Businesses that Automates Money Laundering

Threat actors have intricately crafted a sophisticated application known as XHelper which functions as a crucial tool for efficiently managing a network of money mules. It serves as the technological backbone for fake payment gateways used in various scams, such as Pig Butchering , Task scams , Loan scams, E-Commerce scams, Illegal gambling apps, etc. The app is distributed through websites posing as legitimate businesses under the guise of "Money Transfer Business."

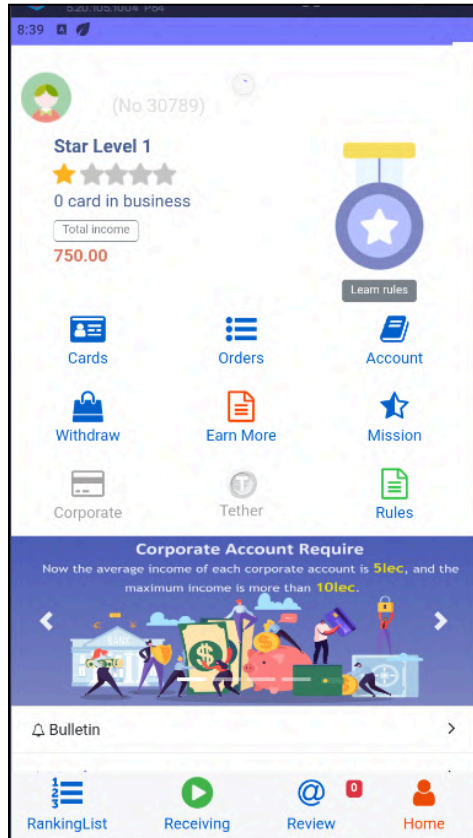


Image Showing Xhelper dashboard

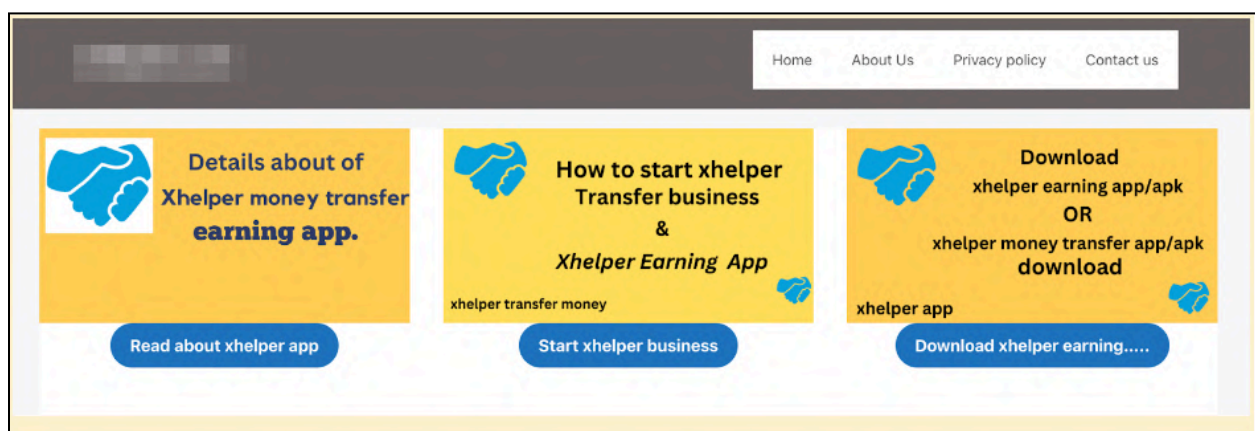
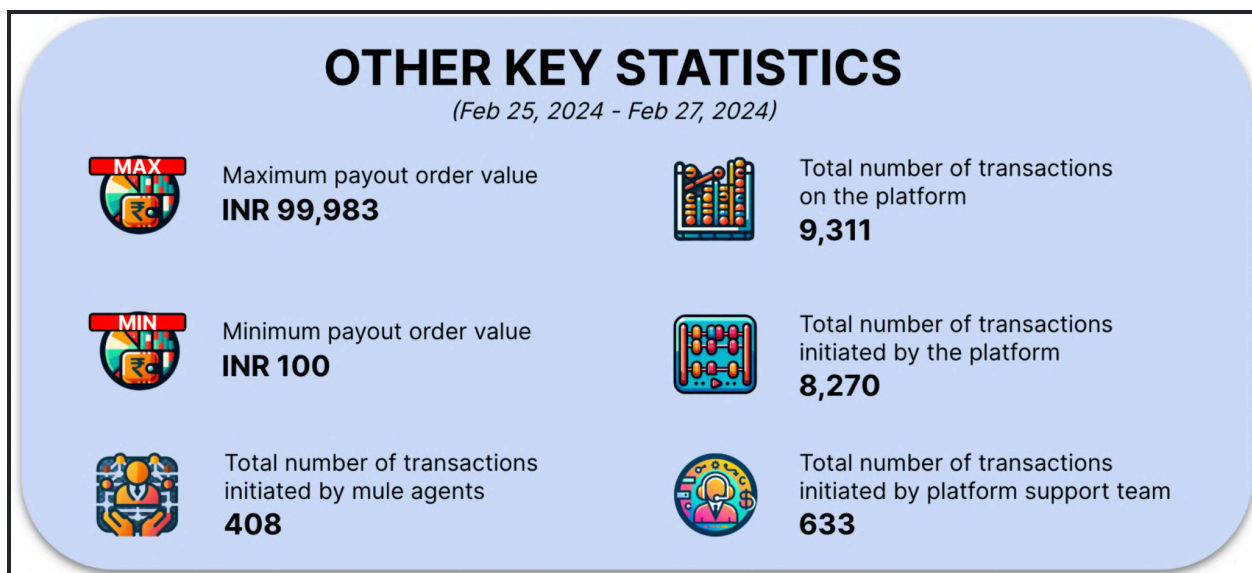
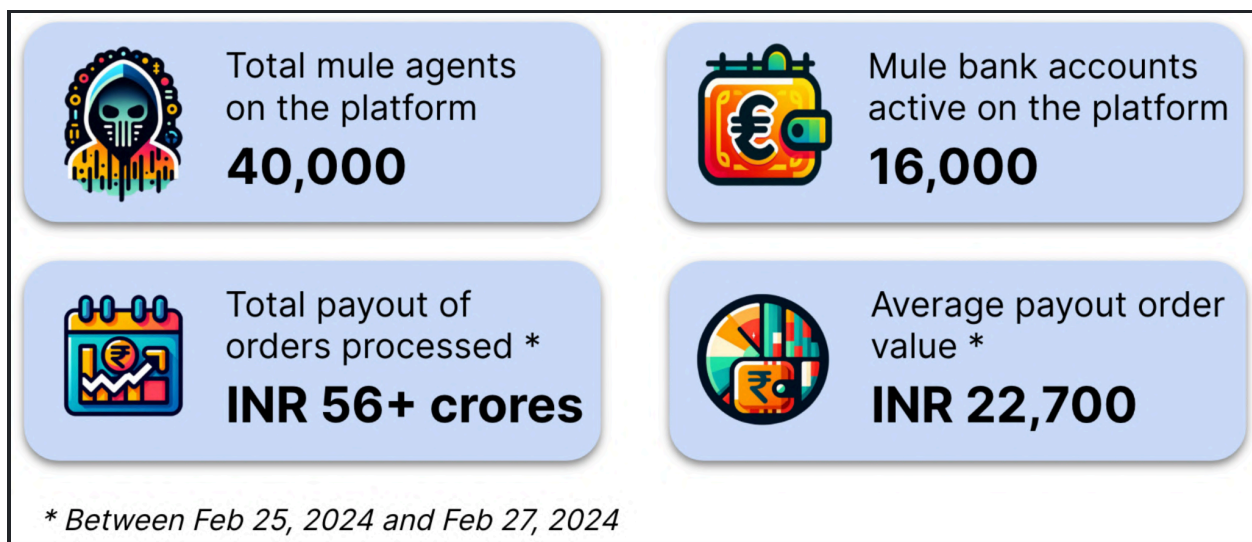


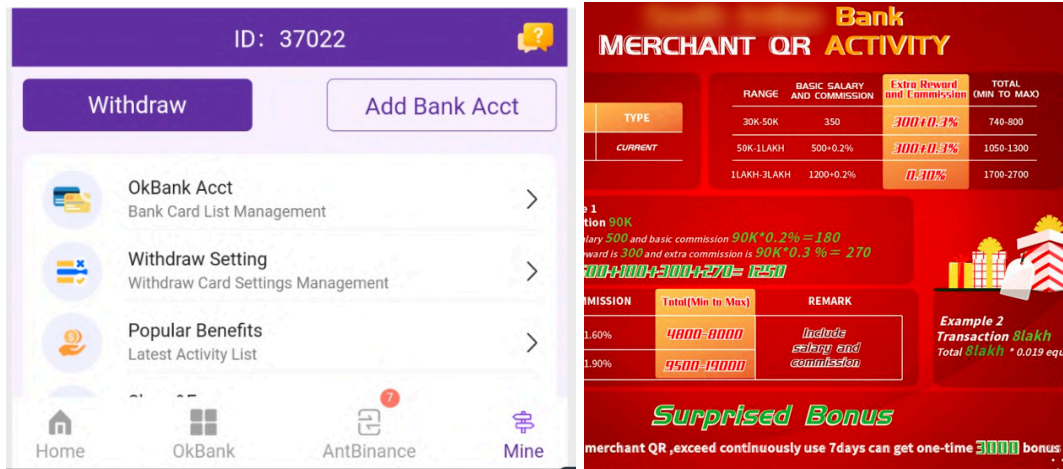
Image showing how threat actors advertise their business

Funds transferred from mule accounts undergo a complex process, reaching threat actors who convert the funds into cryptocurrencies. After deducting their commission, threat actors pay scammers in USDT. Mules also have the option to receive their commissions in USDT.

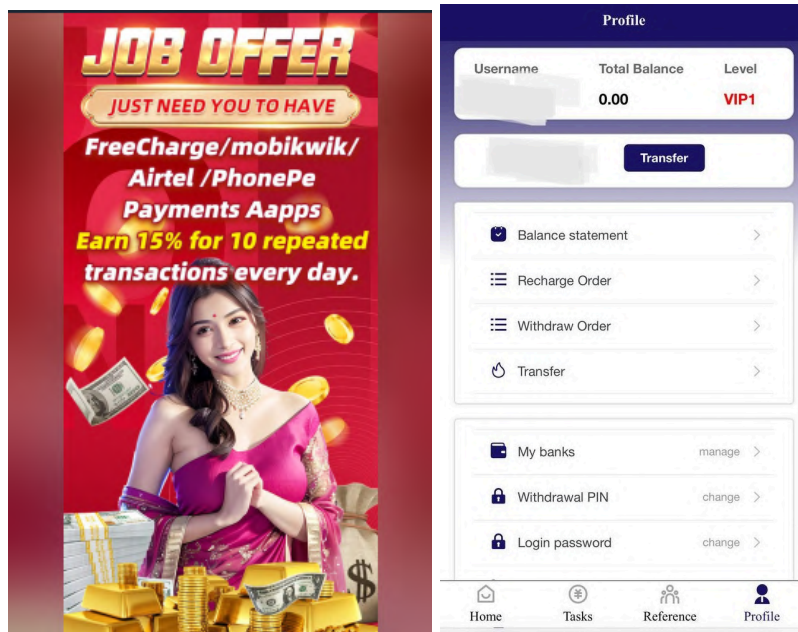
The XHelper app offers various features, including a ranking list for mules to track earnings and compete with others. Additionally, the app incorporates a dedicated support system operating through the binding of Telegram accounts to the APK.



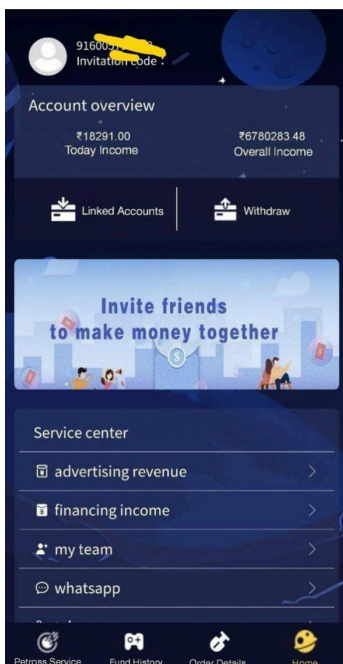
While XHelper serves as a concerning example, it's crucial to recognize this is not an isolated incident. CloudSEK's investigations have revealed a growing ecosystem of similar applications facilitating money laundering across various scams.



Other apps like Xhelper dashboard and being advertised in underground channels



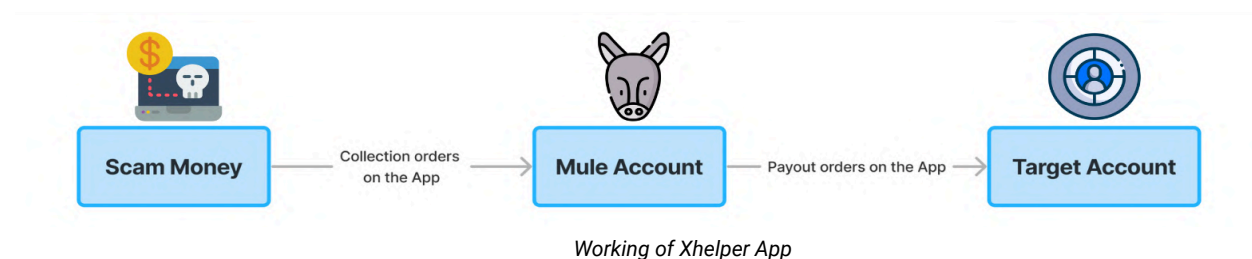
Other apps like Xhelper dashboard and being advertised in underground channels



Other apps like Xhelper

Exclusive Working of XHelper APK

The XHelper app functions as a central hub for malicious money mules, streamlining the execution of illegal financial transactions. Designed for user-friendly operation, the platform simplifies both payout and collection processes, making it an attractive tool for individuals seeking illegitimate profit.



Collection Orders (Passive Role):

- Collection orders within XHelper involve the acquisition of funds or assets, often through fraudulent activities orchestrated by external actors.
- Importantly, money mules do not directly participate in collection activities. Instead, they passively receive incoming funds from scammers utilizing the XHelper platform.

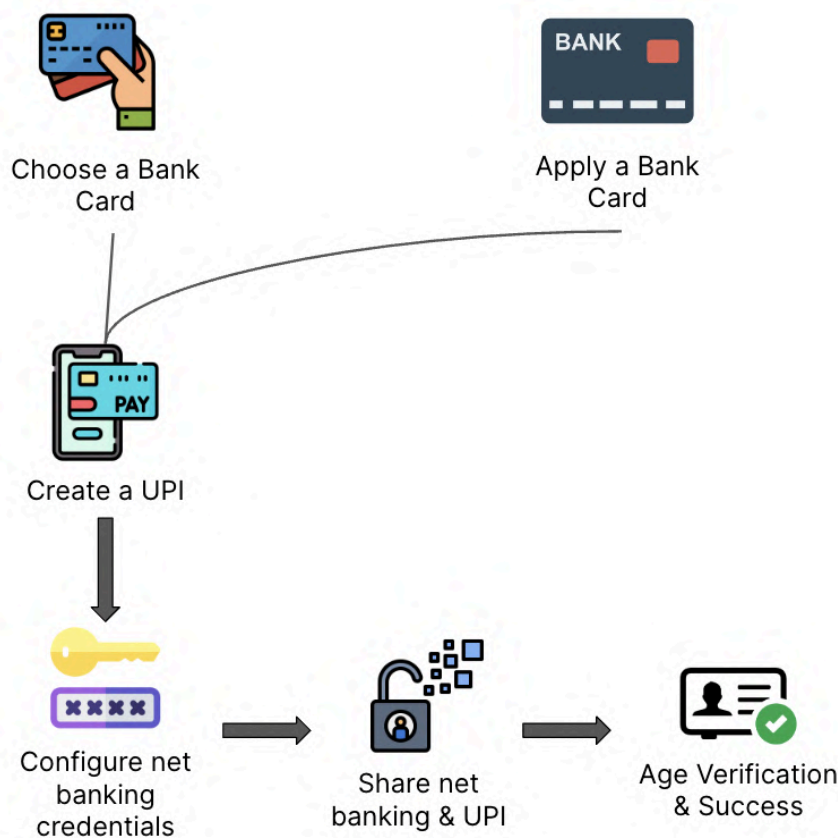
Payout Orders (Active Role):

- Payout orders within XHelper demand the active participation of money mules. These orders mandate the swift transfer of funds to pre-designated accounts within strict timeframes.

- Essentially, these outgoing transactions from mule accounts to the app operators mark the final stage of the illicit financial cycle facilitated by XHelper.

Onboarding and Initial Setup

- Money mules begin by entering their net banking and UPI information within the app. This grants the app access to transfer funds directly into their UPI account.



Initial steps for Money mules for onboarding on the app

New Member Guide

Every new member need to finish the missions in the guide,after that you can go in to the real home page.

allEarnings: ₹750.00

Congratuations !

You have upload your bank card and earn ₹650. Now finish these **last steps** in the new member's guide, you will real begin your work.

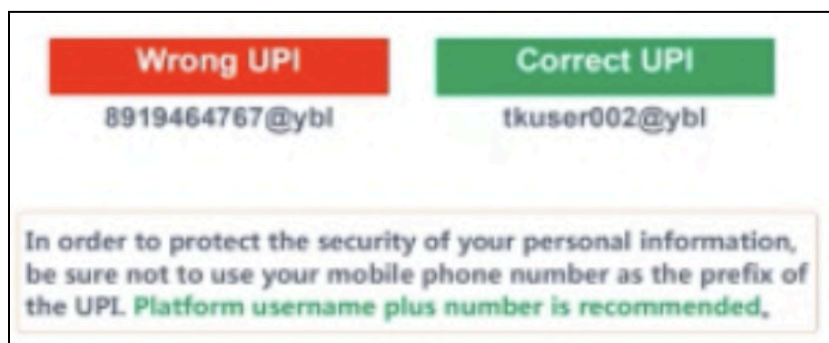
If your bank card is not approved ,click here
 If your Aadhaar Card is not approved ,click here

Adding a banking details are essential for money mules to gain access to the app

Key Operational Instructions for Money Mules during Onboarding

Pattern of UPI address:

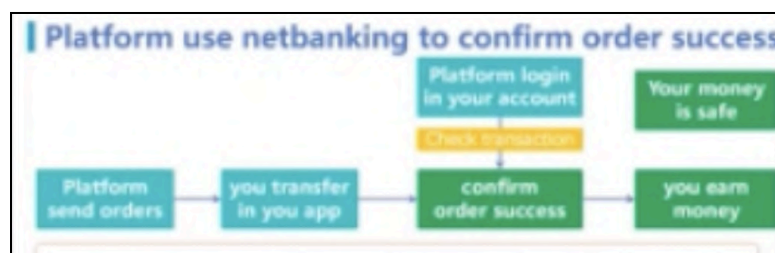
- The individuals acting as money mules are asked to register UPI in a specific format. The format includes the username of the mule on the app. This is because the app is using these UPI addresses in a programmatic way to assign orders.



Money mules are asked to register UPI in a specific format

Net Banking Credentials

- The app in the backend uses net banking to confirm the success of the payout order. Hence it is advised to money mules to ensure that the credentials they are sharing for net banking are correct.



Money mules advised to ensure correct net banking credentials

- The individuals acting as money mules are asked to not change the password associated with the net banking.

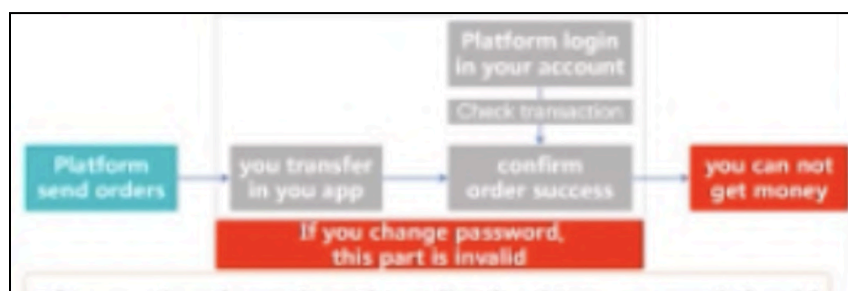


Image showing how Money Mules are Advised Against Password Change

Link to a video from Xhelper app's LMS, providing Key Operational Instructions for Money Mules during onboarding attached [here](#).

Order Processing Workflow for Money Mules on App

Initiation:vcv

- Money mules activate order intake within the XHelper app, enabling them to receive and fulfill money laundering tasks.
- The system automatically assigns orders, potentially based on pre-determined criteria or mule profiles.

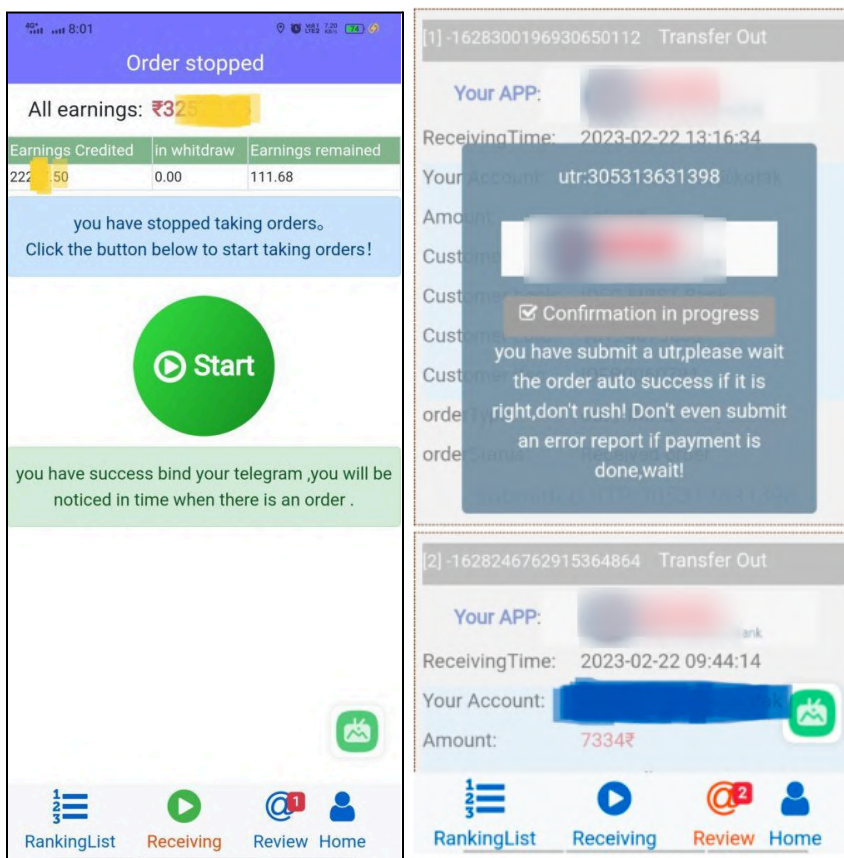


Image showing the activate and process order functions in the mule app

Order Processing:

- Upon receiving a payment order notification, mules review the details (likely containing source, destination, and amount information).

- Following strict adherence guidelines to minimize detection, money mules execute the illicit fund transfer using their linked bank app.

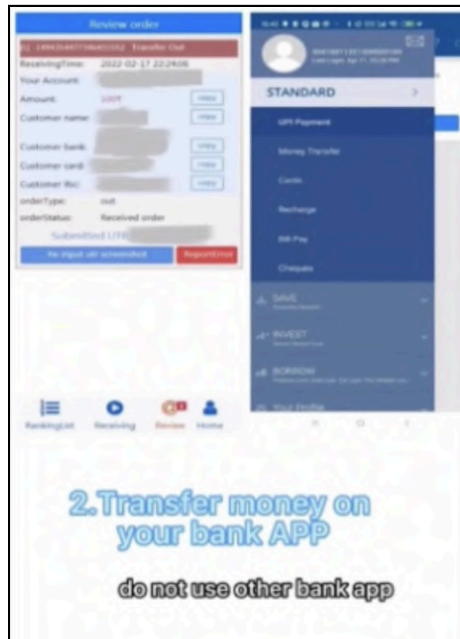


Image Showing how order money mules use bank app to to minimize detection

Verification and Reward:

- After completing the transfer, mules capture and upload screenshots as proof of execution, indicating success or error.
- The XHelper system or designated team automatically verifies the screenshots, streamlining the order validation process.
- Successful order completion translates to financial rewards within the app, incentivizing continued participation.

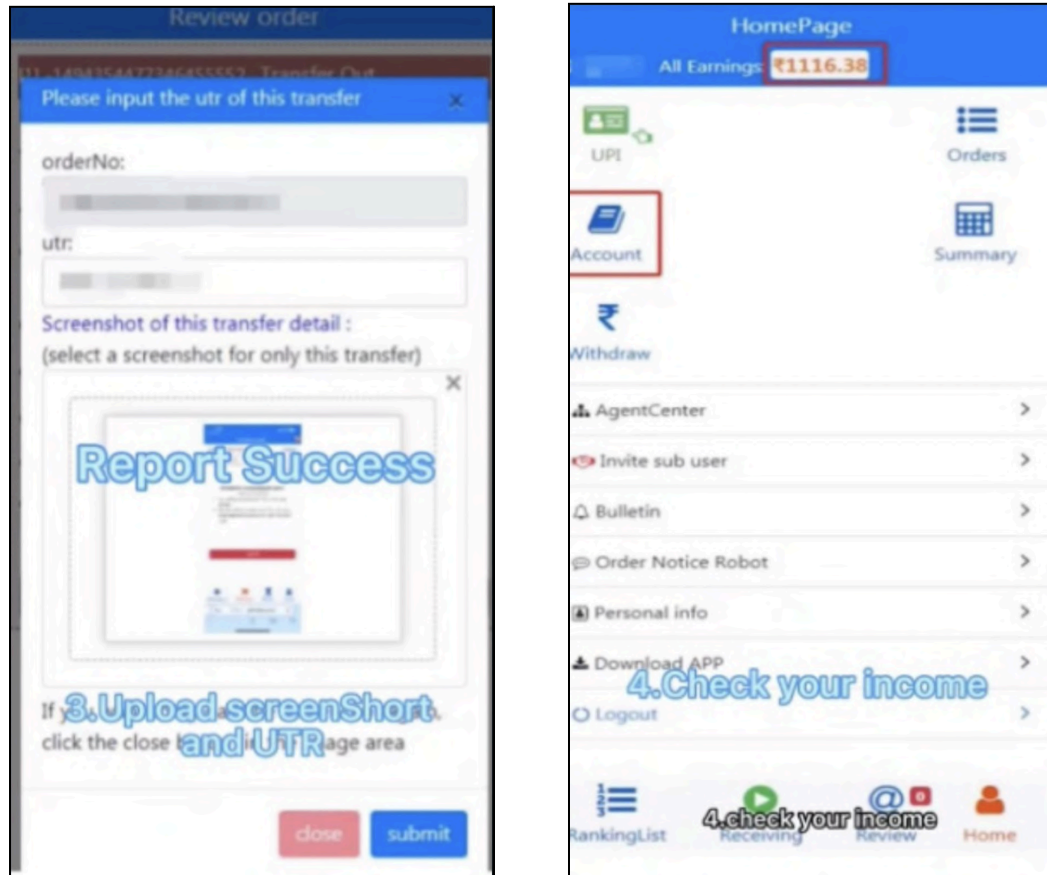


Image Showing how money mules are rewarded after every successful order completion

Link to a video from Xhelper app's LMS on Order Processing Workflow for Money Mules on App attached [here](#).

Key Operational Instructions for Money Mules while Processing Orders

Transfer of OTP (One time password):

- The individuals acting as money mules are presented with two alternatives for submitting a One Time Password (OTP), known as "OTP work" and "No OTP work."
- In OTP work, the money mule can either manually send the SMS to the Mule to finalize the transaction, or the Mule agent offers an application that automatically forwards SMS for all outgoing transactions.
- On the other hand, in No OTP work, the money mules alter the mobile number linked to the Mule account to match the agent's mobile number.

Order Completion Timeframe:

- **Time-Sensitive Rewards:** Money mules are incentivized to complete payout orders within a strictly enforced 10-minute window. Faster processing translates to higher commissions and rewards, promoting rapid and potentially reckless transaction behavior.

Bank Account Selection:

- **Matched Bank Application:** To avoid raising red flags and incurring potential penalties, mules are instructed to strictly use the bank app corresponding to the assigned order. This implies the app might track or verify linked accounts.

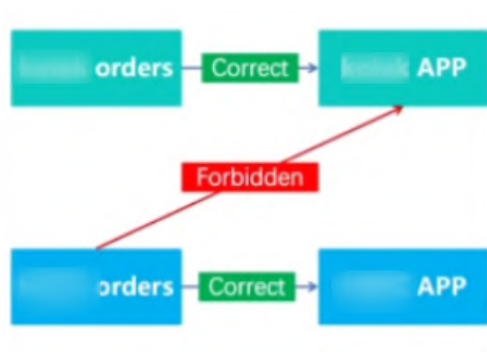


Image Showing how money mules are instructed to strictly use the bank app

Payment Method Prioritization:

- **IMPS/UPI Preference:** Based on the order type, the XHelper app prioritizes specific payment methods, likely IMPS or UPI. This suggests potential order variations and targeted use of specific financial channels to obscure transactions.

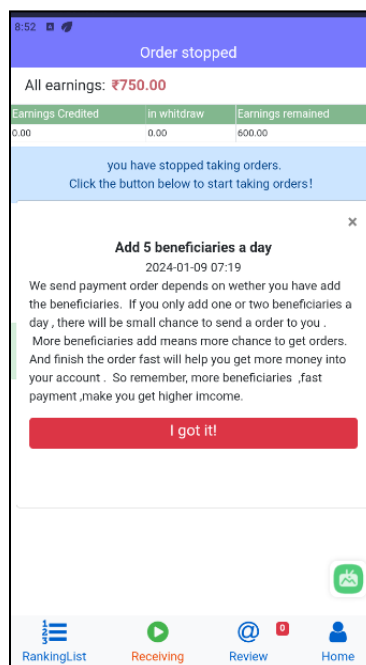


Image Showing encouraging money mules to add beneficiaries

Recruitment of Money Mules

Money mules, recruited by individuals called "Agents," operate within a network established through multiple Telegram channels. Agents pose as thriving businesses seeking efficient fund management due to a high transaction volume. The recruitment often occurs through personal connections, with recruiters or agents persuading individuals in their social circles. Crucially, these so-called mules show a distinct preference for corporate bank accounts, which typically have higher transaction limits. This strategic choice allows the illicit network to move large sums of money more efficiently, maximizing the potential gains from their criminal activities.

The xhelper app incorporates an invitation feature:

Referral System: Agents can invite others to join as agents.

Bonuses and Rewards: Referring agents earn bonuses for each successful recruitment.

This referral system follows a pyramid-like structure, fueling mass recruitment of both agents and money mules, amplifying the reach of illicit activities. Agents, in turn, recruit more mules and invite additional agents, perpetuating the growth of this interconnected network.

11:38 AM

Before invite subline

What you need to do

1.You need to objectively introduce our platform to your subordinates and tell them how you make money.

2.You need to help your subordinates avoid making mistakes and do their jobs well.

3.You are not allowed to ask for any extra money from your subordinates, if found out you will be fired

4.If your subordinates steal money from the platform, you will be responsible for it

Rewards you can get

1.You can get 3000Rs rebate for each cards of your subline.

2.You can apply to be a "mentor" after you have 3 valid sublines , then you can get 5000Rs-9000Rs rebate for each cards of your subline.

3.You can get rebate from your subline's usdt transactions

4.You can get 25% of your subline's first two corporate's bounty and enjoy other corporate invite prize.

11:12 AM

Akash9336

card Id: bank bankCardCode rebate from platform

38181 HDFC 50100677681461 0

Zepto1234

card Id: bank bankCardCode rebate from platform

38858 HDFCNew 50100672129152 1478.5

45199 Federal 55550114933185 0

45859 Federal 24860100002624 0.41

46020 Federal 24860100002624 845.51

Ankit859

card Id: bank bankCardCode rebate from platform

46742 kotak 3648819188 0.4

Parvaiz786

card Id: bank bankCardCode rebate from platform

Gouri860

card Id: bank bankCardCode rebate from platform

Nikhilxx

card Id: bank bankCardCode rebate from platform

Ibrahim258

card Id: bank bankCardCode rebate from platform

11:40 AM

deduct type platform acct id sub user name

personal_card 27809

lost amount need deduct amount status

20533 20533 all_deduct

real deduct amount remark

20533

deduct type platform acct id sub user name

sub_rebate 26402 Rapido1235

lost amount need deduct amount status

59786.7 2075.72 all_deduct

real deduct amount remark

2075.72

deduct type platform acct id sub user name

sub_rebate 19327 Omkarjadhav

lost amount need deduct amount status

224.19 3282.46 all_deduct

real deduct amount remark

3282.46

deduct type platform acct id sub user name

sub_rebate 22492 Omkarjadhav

lost amount need deduct amount status

118.18 5000 all_deduct

real deduct amount remark

5000

deduct type platform acct id sub user name

sub_rebate 23640 Omkarjadhav

lost amount need deduct amount status

11894 58.88 all_deduct

Inviting process and managing money mule agents by the top level Mule agents

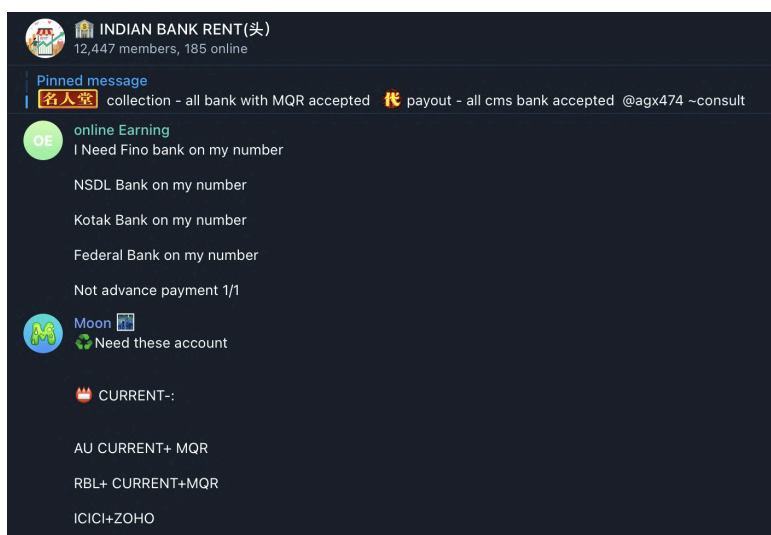


Image Showing how Mule Agents recruit Money Mules on Telegram

Link to a video from Xhelper app's LMS showing money mules referral system attached [here](#).


Training of Money Mules

Learning Management System (LMS) for the XHelper APK, an app used by cybercriminals to onboard money mules provides a concerning glimpse into their recruitment and training tactics.

- **Target Audience:** Money mules recruited to launder stolen funds using their bank accounts.
- **App Functionality:** XHelper app facilitates uploading bank and UPI details, processing orders (likely money laundering transactions), and withdrawing "earnings."
- **Content Focus:**
 - Streamlining money laundering process (uploading cards, processing orders).
 - Maximizing profits (adding more cards, strategic card usage).
 - Justifying activity (showcasing success stories, addressing concerns).
 - Overcoming obstacles (handling frozen accounts, exceeding limits).
 - Handling cryptocurrency transactions (using USDT on Binance P2P).
- **Overall Goal:** Induce new recruits and equip them to efficiently launder stolen funds through the XHelper app.

Learning

video	watch	assess
platform introduction	✓	
how to upload UPI&bank card	✓	
how to withdraw	✓	
how to process orders	✓	
upload more bank card to make more money		Go
Real cases of members making money		
New Member Must Know		
workflows Introduction		
Daily Work Orders Rules		
How to open high limit and not easy frozen card		
How to reasonable to use bank card to prevent easy freeze		
Solutions to increase commission		
More Money-Making Opportunities		
Documents required to open corporate account		
Questions you care about about the Corporate account		
how to do USDT transaction in xhelper	✓	
How to Buy USDT on Binance P2P		
Questions you care about about the USDT transaction		
What to do if your account is frozen		
Limit Excess Solution		
Lien Hold Problem Solution		
Cyber Complain Solution	✓	



What I share with you today is the account opening policy of AXIS

Account opening requirements:

1. Personal account: Proof of identity (PAN card, Aadhaar card, etc.) and proof of address are required.
2. Minimum opening deposit: - INR 1000 for personal account

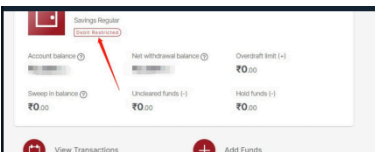
Account opening process:

1. Fill out the account opening application form at the AXIS branch and submit the materials.
2. Bank conduct KYC verification and material review.
3. After passing the review, sign the account opening agreement to complete the account opening.
4. Deposit the initial deposit amount for the first time to activate the account.
5. Set up online banking password, open debit card and other services.
6. Door-to-door account opening is also available, and AXIS will provide full service.

Main account opening materials:

- Personal: proof of identity, proof of address, photo, etc.
- First account opening deposit

680 15:39



What to do if debit restricted appears in IDFC bank account?

Common reasons for debit restricted in IDFC include:

1. Insufficient funds in the account

If the account balance is zero or negative, the bank sets a withdrawal limit. It can be canceled after sufficient funds are deposited in the account.

2. No KYC information provided

If identification documents are not submitted in time, bank will restrict account transactions. Updating the complete KYC information can be resolved.

3. Tax Verification

In order to comply with tax regulatory requirements, banks need to conduct regular tax audits on account holders.

4. Court orders

The court may issue an account freezing order due to litigation and other reasons, resulting in restrictions on withdrawals. Subject to court direction.

5. Suspicion of suspicious trading activities

If there are abnormal transactions in the account, the bank may suspend its use. Usually contact the bank to explain the situation can be resolved.

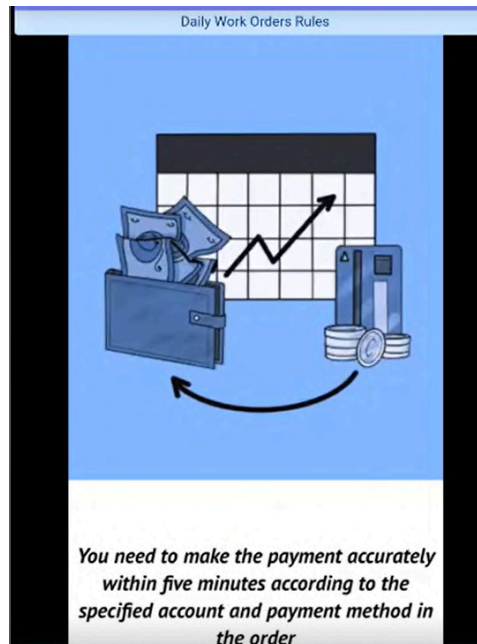
832 16:04

LMS on Xhelper app and tutorials shared by the Agents

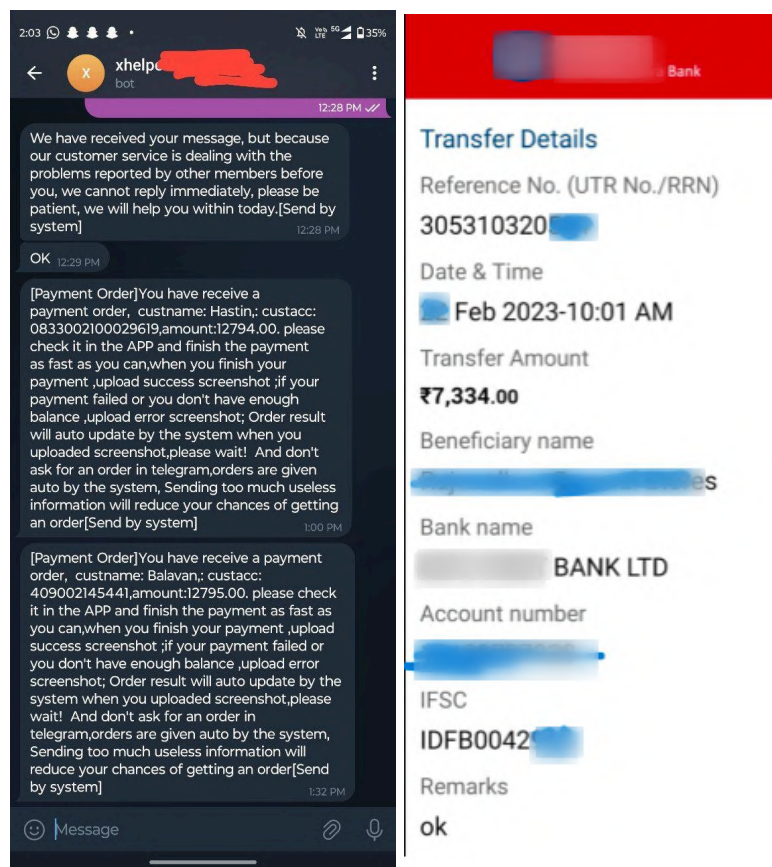
Movement of Money From the Mule Account

Financial Transactions and Fund Transfer Process:

- **Incoming Funds to Mule Accounts:** Mules receive funds in their linked bank accounts through the payment gateway integrated into the XHelper app.
- **Transfer to Corporate Mule Accounts:** Mules are mandated to transfer the received funds to specific predetermined corporate mule accounts within a stipulated time frame, typically around 10 minutes. These corporate accounts, controlled by the XHelper application providers, have higher transaction limits.



Mules must quickly transfer received funds to specific corporate accounts within about 10 minutes



Mules transferring the incoming payments to xhelper owned accounts

- Preventing Accumulation in Mule Accounts:** The time-sensitive nature of the fund transfer aims to prevent the accumulation of funds in individual mule accounts. This ensures that the application providers are not defrauded by the mules.

orderNo: 1629794010421788672 [succ]	
receiveTime	submit utr time
2023-02-01 10:00:00	2023-02-01 10:00:00
order Amount	real payment
11560	11560
pay minute	bounty discount
3	100%

orderNo	type	amount	balance
1629794010421788672	plus_bounty	100.00	8971.45
1629794010421788672	bounty	115.60	8871.45
1629722011116765	punish	-100.00	8755.85
1629687174116933	bounty	30.00	8855.85
1629649310696079	bounty	18.00	8825.85

Mules getting paid and punished based on how fast the incoming money is transferred to Xhelper owned accumulator accounts

- Transfer Mechanism to Application Providers:** Funds transferred from mule accounts are directed to dedicated accounts provided by the threat actors or application providers. These accounts are added as beneficiaries by the mules for performing IMPS transaction, enabling swift and controlled fund transfers.

Daily Work Orders Rules

Order stopped

All earnings: ₹154116.16

Earnings Credited	in withdraw	Earnings remained
101769.00	10000.00	8364.09

you have started taking orders.
Review and successfully complete the received orders in time, the system will give more orders to you, then you will get more income

Important

In order to get more orders, your bank card need to add some beneficiary, go to the upi page to see details and add beneficiary in you bank APP.

Missing this step will make you lost the chance of making more money.

[Go to UPI page to add beneficiary](#)

[click here](#)

Daily Work Orders Rules

BankCard&UPI

[maximum number of cards is relative to deposit]

[+ Click here to add bankCard&UPI](#)

Your bankCard&UPI list

26655: Indusind-Chandan Kumar Mandal-

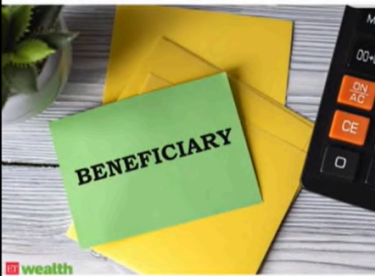
bank card	CustomerId	password

ifsc	status	addDate
	available	2023-07-09 18:15:01

[Click here add beneficiary to this card](#)

[click here](#)

Daily Work Orders Rules



You should add all the beneficiaries sent to you by the system because only by adding beneficiaries can you proceed higher IMPS transactions and earn higher commissions

Mules are instructed to add dedicated accounts as beneficiaries for controlled transactions

- Crypto Conversion and Commission Deduction:** The funds transferred out from the mule accounts are sent to threat actors, who subsequently convert this money into cryptocurrencies. After deducting their commission, threat actors remunerate scammers in USDT, a stablecoin pegged to the US Dollar.
- Mule Commissions in USDT:** Mules, as active participants in the illicit financial operations, have the option to receive their commissions in USDT. This adds a layer of anonymity to the transactions, as cryptocurrencies provide a degree of privacy.



Mue agents offering to pay the commissions in USDT and INR

Link to a video from Xhelper app's LMS showing movement of money from the mule account attached [here](#).

Earnings of Money Mules on App

The app employs a hierarchical structure for mules, with new mules initially limited to adding up to 2 banks. mules can increase their limits through leveling up, based on their performance, unlocking additional commissions and benefits

Username	Total Income
shahbaz	12,714,545.27
Register26	12,536,179.90
Ranjan1982	12,199,516.30
Shailendar	10,123,620.57
Rakamsingh	9,461,049.48
zycorp01	8,080,689.07
Narshima	6,378,690.46
koushik8016	6,242,319.87
Arpanadevi	6,049,542.31
RAMKABIR77	5,577,885.92


Level	Performance	Daily allowance	Transaction reward
 V1	>0	350	0.00%
 V2	>50000	500	0.20%
 V3	>100000	1200	0.22%
 V4	>300000	1800	0.24%
 V5	>500000	2000	0.26%
 V6	>1000000	0	0.28%
 V7	>3000000	0	0.29%
 V8	>1 crore	0	0.30%


App Hierarchy for Mules Unlocking More Banks, Commissions, and Benefits with Performance Levels

For example

You have 5 bank cards

Each bank card earned 55000 yesterday

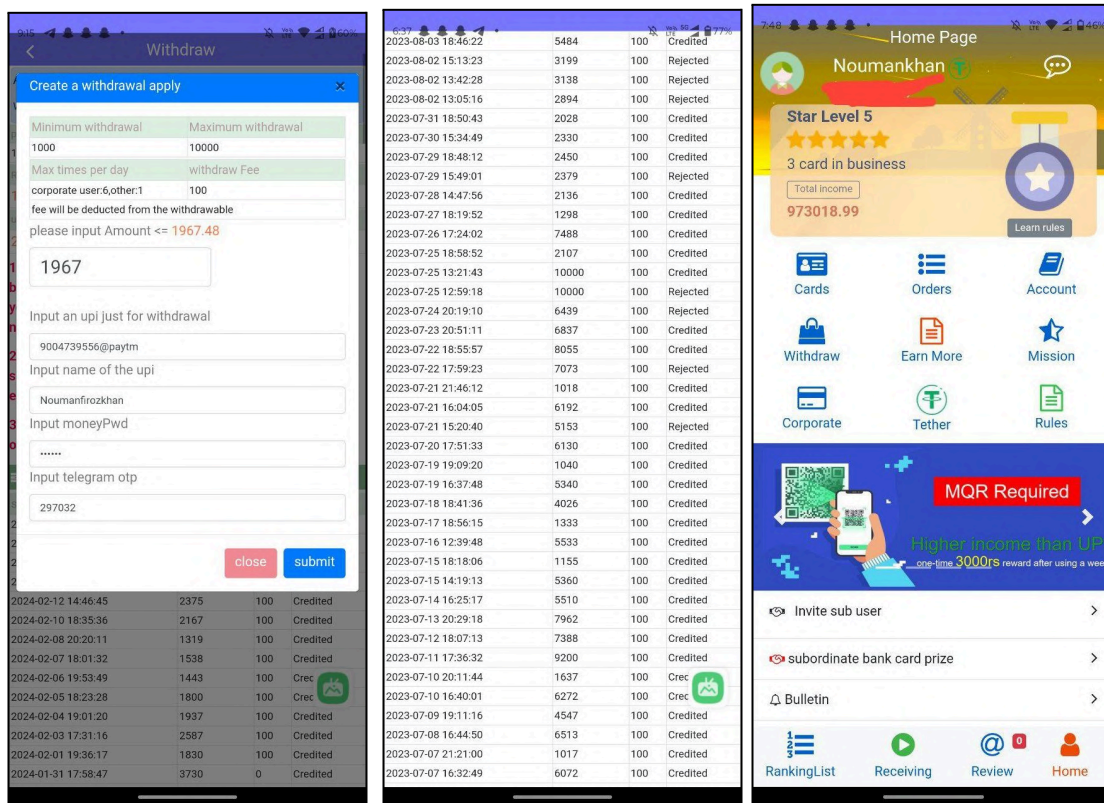
Your daily allowance =  V2 = 500 * 5 = 2500

So it's 5 * 55000 = 275000 =  V3 = 27500 * 0.22% = 605

Your total income is 2500 + 605 = 3150

level	Per Account Daily Total Transaction	Daily Salary
Basic	3k-50k	350
Starters	50k-1akh	500
Red Bull	1lakh-3lakh	1200
Royal Challengers	3lakh-5lakh	1800
Mumbai Express	5lakh-10lakh	2000

Daily Earnings of Money Mules on App



Mule Agents showing proofs of the amount of money that flows through each agent

Link to a video from Xhelper app's LMS showing how mules can earn money within the app by adding an additional bank account attached [here](#).

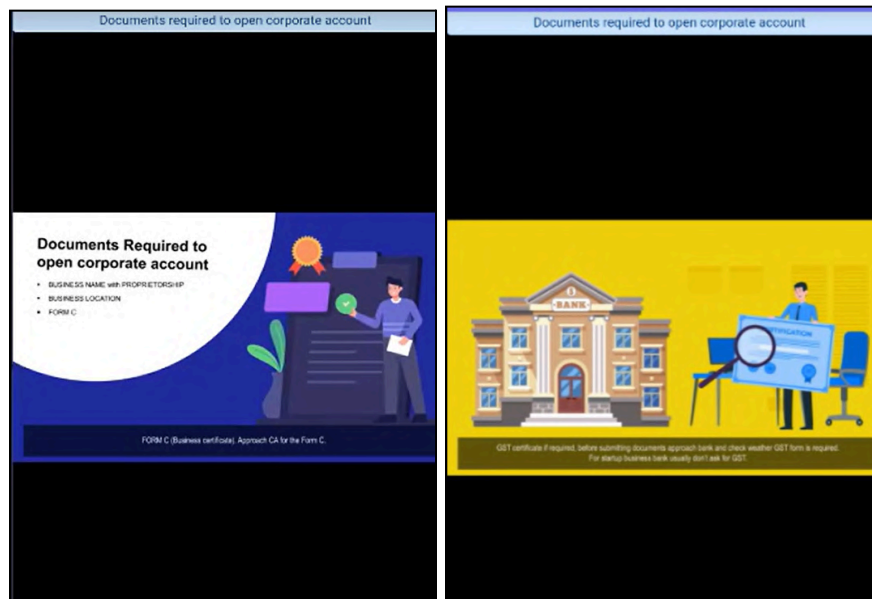
How Money Mules Open Fake Corporate and Merchant Accounts

Agents and money mules demonstrate a distinct preference for corporate and merchant bank accounts. This preference is driven by the higher transaction limits associated with corporate accounts. Corporate accounts offer greater flexibility, enabling the processing of larger sums of money. The allure of these accounts lies in their capacity to accommodate substantial transactions, making them particularly attractive for the illicit activities conducted through the money mule network.

The Xhelpers app provides LMS training for money mules on opening corporate/merchant accounts. The process involves:

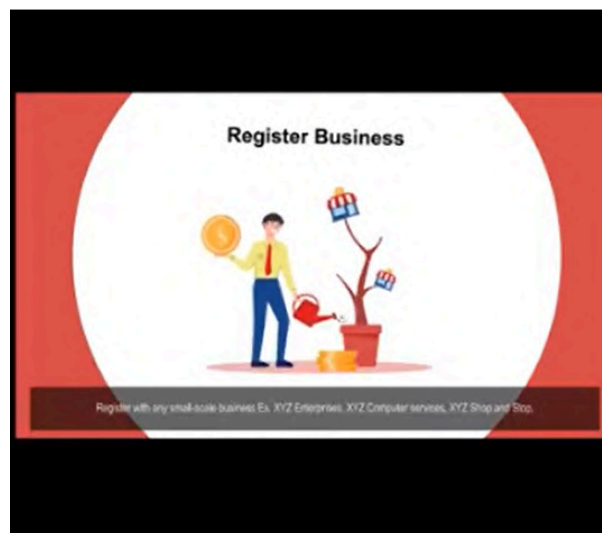
1. Obtaining necessary documents:
 - Business name with proprietorship
 - Business location
 - Form C (advising to consult a CA)

- Verifying the need for a GST certificate with the bank, suggesting consulting a CA if required (takes up to 4 days)



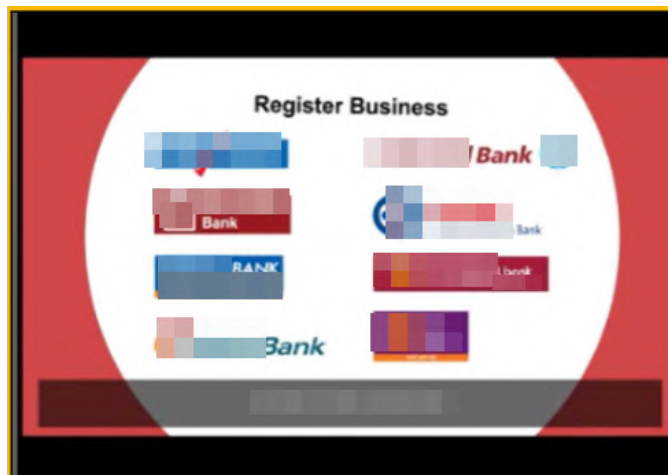
Necessary documents required for opening corporate accounts

2. Registering KYC Aadhar card and PAN card with suggested small-scale businesses (e.g., XYZ enterprise, XYZ computer services, XYZ shop and stop).



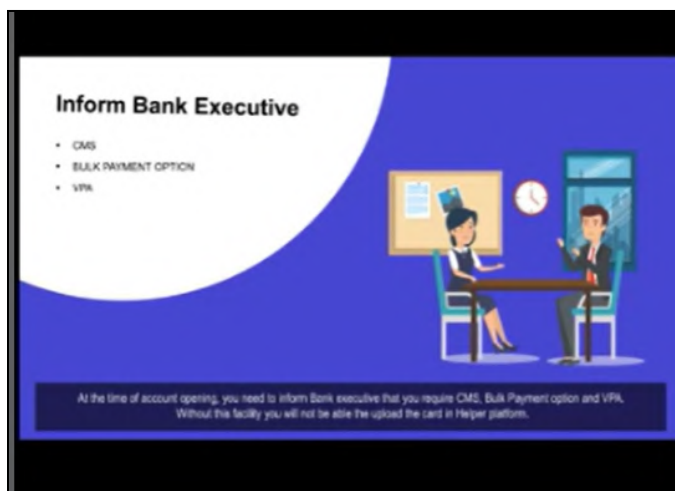
KYC Registration with Small-Scale Businesses is suggested for money mules

3. Submitting all prepared documents to the bank, with recommended banks provided by Xhelpers.



Recommended banks suggested by Xhelper app

4. Instructing money mules to inform bank executives about specific requirements for app access:
 - CMS
 - Bulk payment option
 - VPA

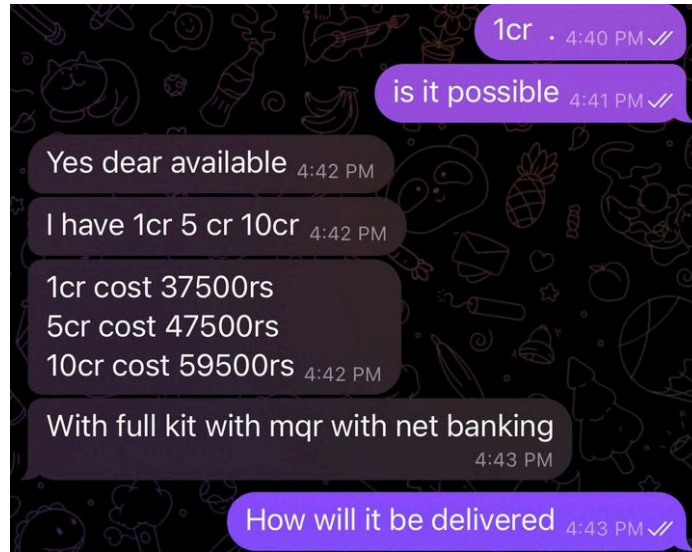


Instructing money mules to inform bank executives about specific requirement while creating corporate bank account

5. Emphasizing the potential for high daily income by uploading their corporate account information to the app.

Besides the guidance provided by Xhelper training, money mules and agents also purchase accounts with higher limits, equipped with net banking and MQR, through Telegram.

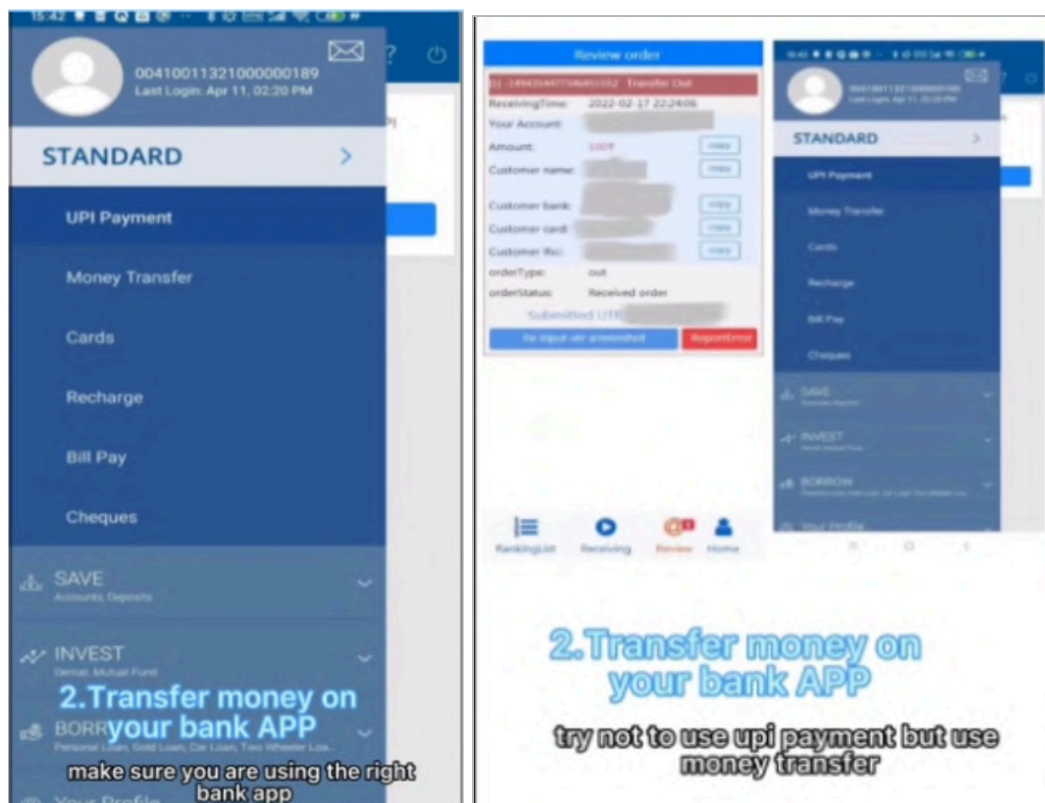
Link to a video from Xhelper app's LMS showing how money mules are taught to open fake corporate and merchant accounts within the app is attached [here](#).



Sensitive source contacted agents selling bank accounts with higher limit

DavalWhy Money Mule Apps Favor Bank-Specific UPI Applications

- **Stealthy Transactions:** Bank UPI apps provide scammers with a platform for conducting transactions discreetly, mitigating the risk of immediate detection or suspicion by leveraging the relative lack of visibility associated with bank-specific platforms.



- **Bypassing Third-Party Monitoring:** The choice of bank UPI apps allows scammers to circumvent potential monitoring mechanisms associated with popular third-party applications. This avoidance of third-party oversight enhances the scammers' ability to involve money mules in unauthorized transactions without triggering immediate alerts or security measures.
- **Perceived Lower Security Standards:** Money mules may perceive bank-specific UPI apps as having lower security standards compared to well-established third-party platforms. Scammers exploit this perception to encourage money mules to adopt bank apps, fostering an environment where fraudulent activities can occur with a diminished risk of detection.
- **Mitigation of Account Blocking Risk:** Scammers are cognizant of the potential consequences of account blocking by popular third-party services. Advising the use of bank applications allows them to strategically lower the risk of account suspension, providing a more sustained opportunity for money mules to execute fraudulent transactions before intervention.

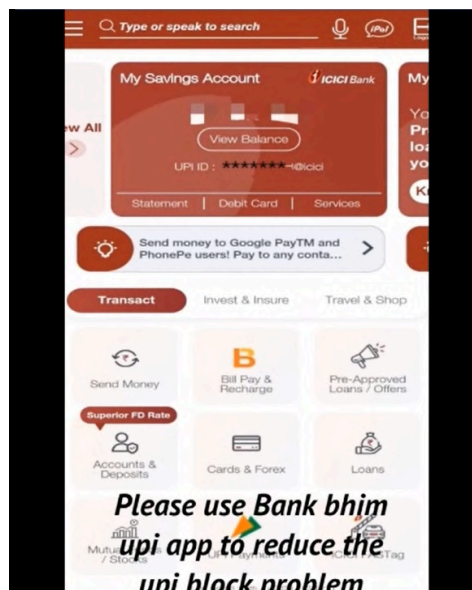


Image Showing encouraging money mules to use Bank UPI apps

- **Reduced Suspensions:** Money mules and authorities may be more accustomed to transactions through bank apps, potentially leading to reduced suspicions. Scammers may exploit this familiarity to involve money mules in their fraudulent activities with a lower likelihood of raising alarms.
- **Payout Order Verification via Net Banking:** Scammers favor bank apps because they utilize net banking to receive automated confirmations upon the completion of payout orders.

Strategies Employed by Money Mules to Bypass Account Freezes

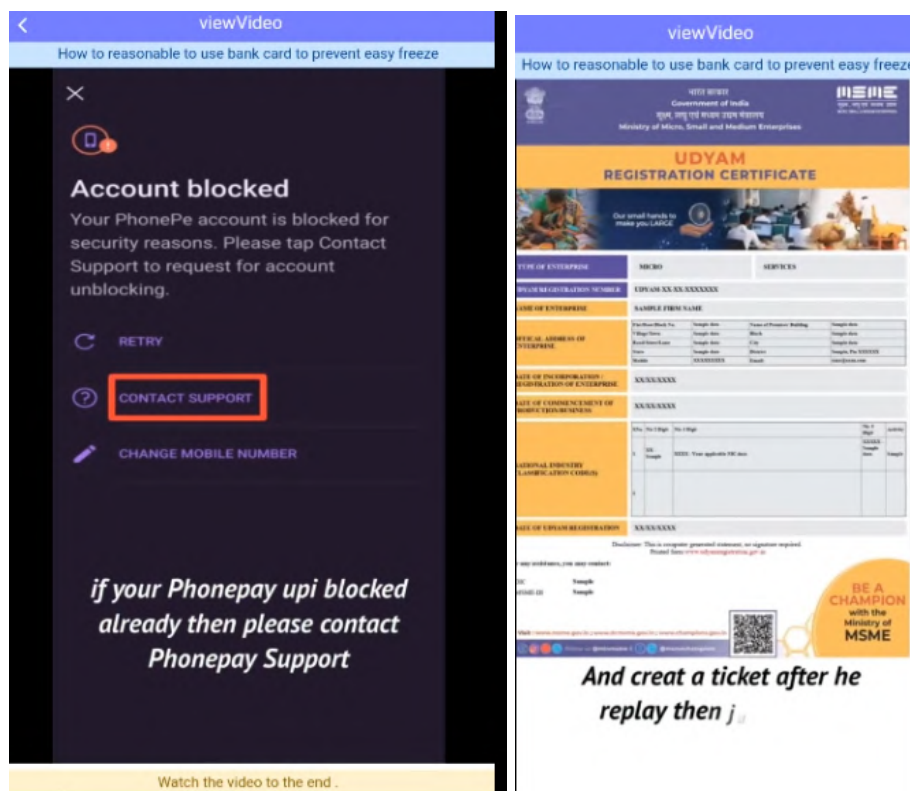
Despite law enforcement efforts and frozen accounts, agents constantly devise methods to circumvent these blockages, enabling money mules to continue their illicit activities.



Image Showing authoritative notice received by mule

When a mule's UPI is already blocked by PhonePe or Google Pay, they are advised to take specific steps to address the issue:

- **Contact Support Through App:** Mules are instructed to contact support through the respective app and create a ticket to unblock the UPI.
- **Provide Business Proof:** Once the support executive responds, mules are required to provide business proof, including Udyam, GST, trade license, and PAN card.
- **Wait for 24 Hours:** After submitting the necessary documents, the UPI apps are expected to unblock the UPI within 24 hours.



Mule mules showing how they can Unblock the blocked UPI

However, if the UPI support apps do not respond or the UPI is not unblocked:

- **Visit the Bank:** Mules are advised to go to the bank and request unblocking the UPI. Before doing so, scammers are encouraged to check their daily transaction limit to confirm whether the freeze was due to transaction limits.
- **Use Current Accounts:** Current accounts are recommended as they are less prone to freezing compared to saving accounts, which have fewer features and a shorter lifespan.


Training for Bank Customer Support Calls:

- **Bank Customer Support Communication:** Mules undergo training to communicate effectively with bank customer support in response to suspicious transactions. When called for security reasons, mules provide information such as their real name (answered with the mule account name), purpose of transactions (sending money to a friend), self-execution of the transaction (answered with yes), transaction method (net banking using IMPS mode), and familiarity with the beneficiary.
- **Verification Process:** During bank customer support interactions, mules may encounter questions regarding the amount being transferred, date of birth, and mother's name for

verification purposes. It is crucial for mules to respond accurately to maintain the appearance of legitimacy in their transactions.

viewVideo

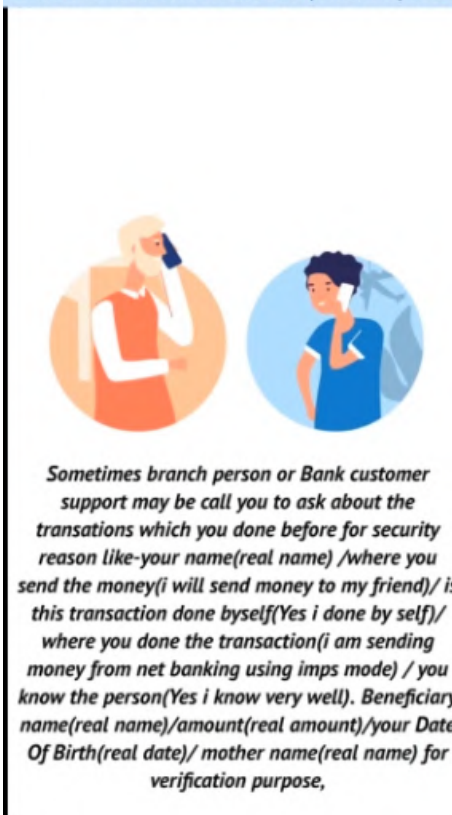
How to reasonable to use bank card to prevent easy freeze



Please check your daily limit on your account sometime it will be reach and very easy to forzen,

viewVideo

How to reasonable to use bank card to prevent easy freeze



Sometimes branch person or Bank customer support may be call you to ask about the transations which you done before for security reason like-your name(real name) /where you send the money(i will send money to my friend)/ is this transaction done byself(Yes i done by self)/ where you done the transaction(i am sending money from net banking using imps mode) / you know the person(Yes i know very well). Beneficiary name(real name)/amount(real amount)/your Date Of Birth(real date)/ mother name(real name) for verification purpose,

Mule Agents providing training to mules on how to talk with bank employees

Apply for Merchant VPA:

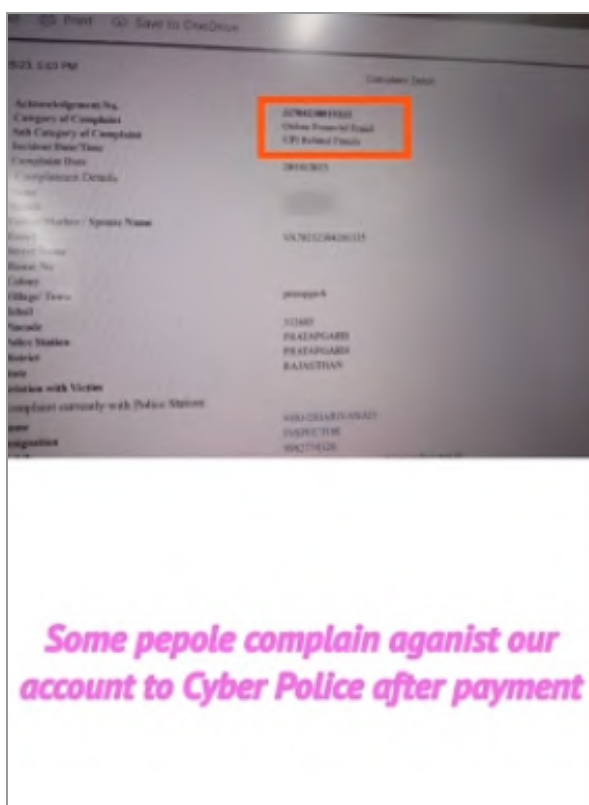
- **Apply for Merchant VPA:** If using a current account or applying for one, mules are advised to visit the bank and apply for a Merchant VPA (Virtual Payment Address). This reduces the chance of UPI getting blocked, as transactions are less likely to be flagged as suspicious.
- **Merchant VPA Application Process:** Mules need to visit a branch, express the need for a merchant VPA for their business (e.g., CSC Center, Grocery Wholesale, Auto Parts, Cement Workshop), provide business proof, and fill out the application form for the merchant VPA. Upon submitting all necessary details, the bank will issue the merchant VPA.

Link to a video from Xhelper app's LMS showing how money mules are guided to Bypass Account Freezes is attached [here](#).

Dealing with Cyber Complaints:

- **Visit Home Branch or Nearest Branch:** Mules are instructed to go to their home branch or the nearest branch where they hold their bank account.
- **Convince Banker:** Attempt to persuade the bank personnel to resolve the issue and lift the freeze on the account.
- **Help Find the Complaint Person:** Work towards identifying the individual who lodged the complaint against the mule.
- **Contact Complainant and Negotiate:** Reach out to the complainant, discussing the issue and attempting to negotiate a resolution. Propose a settlement and express a willingness to rectify any concerns.
- **Provide Complaint Report and Repay:** Present a complaint report to the complainant and repay the claimed amount.

Seek a No Objection Certificate (NOC) after making the repayment.



Screenshots of agents advising mules to pay money and get NOC from the Victim

- **Always Pay Complainant:** Emphasize the importance of settling the payment with the complainant to resolve the issue.

- **Submit NOC to Bank:** Take the NOC obtained from the complainant to the bank and submit it for verification.
- **Bank Verification and Unfreezing:** The bank conducts a verification process and, upon satisfactory results, unfreezes the account.
- **Addressing Unresolved Issues:** If the problem persists, explore the possibility of unresolved disputes or larger legal issues.
- **Understanding Borrowing Situations:** Mules are informed that complainants may borrow money from cooperative customers and later file complaints about collection amounts. This narrative is presented to convince mules that their activities are not illegal.
- **Negotiate Settlement:** In situations involving disputes, mules are advised to reach a settlement with the complainant.
- **Avoid Arguments with Authorities:** Mules are strictly cautioned against arguing with bankers or law enforcement, especially regarding the complaint.



Screenshots from the tutorials shared by the Mule agents

- **Hiring an Advocate:** If needed, mules are advised to engage legal assistance by hiring an advocate to navigate the legal complexities.
- **Never Argue with Authorities:** Mules are firmly reminded never to argue with bankers or law enforcement, particularly when it comes to addressing complaints.

Link to a video from Xhelper app's LMS showing how money mules are taught to deal with cyber complaints is attached [here](#).

Impact on Banks

- **Financial Losses:** Money mule activities can result in financial losses for banks due to fraudulent transactions and compromised accounts.

- **Operational Strain:** Banks face operational challenges in monitoring and preventing money mule activities, requiring additional resources for security measures.
- **Technological Risks:** The exploitation of money mule app capabilities poses technological risks, potentially compromising the security of banking systems.
- **Customer Trust:** Involvement in money mule activities may lead to a loss of customer trust, affecting the bank's reputation and customer relationships.
- **Legal and Compliance Issues:** Banks may face legal consequences and regulatory scrutiny, resulting in potential fines and penalties.
- **Transaction Monitoring Costs:** Enhanced transaction monitoring to detect and prevent money mule activities can increase operational costs for banks.
- **Resource Allocation:** Dealing with the impact of money mule activities requires banks to allocate resources for investigations, security measures, and compliance efforts.
- **International Compliance Challenges:** Money mule transactions involving the international flow of funds create challenges for banks in adhering to cross-border regulatory compliance.

Proactive Measures for Strengthening Bank Controls Against Money Mule Activities

1. **Enhance Merchant Account Opening Procedures:**
 - a. Implement stricter verification protocols to detect forged documents and prevent fraudulent account creation.
 - b. Consider utilizing digital identity verification solutions for a more robust process.
2. **Bolster Netbanking Security Measures:**
 - a. Implement multi-factor authentication (MFA) as mandatory for all netbanking activities, including payment confirmations.
 - b. Monitor and flag suspicious activity involving frequent beneficiary additions or changes.
 - c. Educate users on the importance of secure practices and phishing prevention.
3. **Address Victim Information Sharing:**
 - a. Strengthen data privacy protocols to prevent unauthorized access to victim information.
 - b. Implement stricter procedures for responding to requests for victim data, prioritizing victim protection.
4. **Leverage External Data for Risk Assessment:**
 - a. Explore partnerships with social media platforms or other data providers to gather insights for identifying high-risk users.
 - b. Develop risk scoring models that integrate external data sources to improve real-time detection of money mule activity.

5. Integrate Payment Red Flags in Faster Payments:

- Collaborate with payment service providers to implement red flag indicators within Faster Payment messages.
- Identify suspicious transactions based on pre-defined red flags, such as unusual recipient names, locations, or high-risk payment patterns.

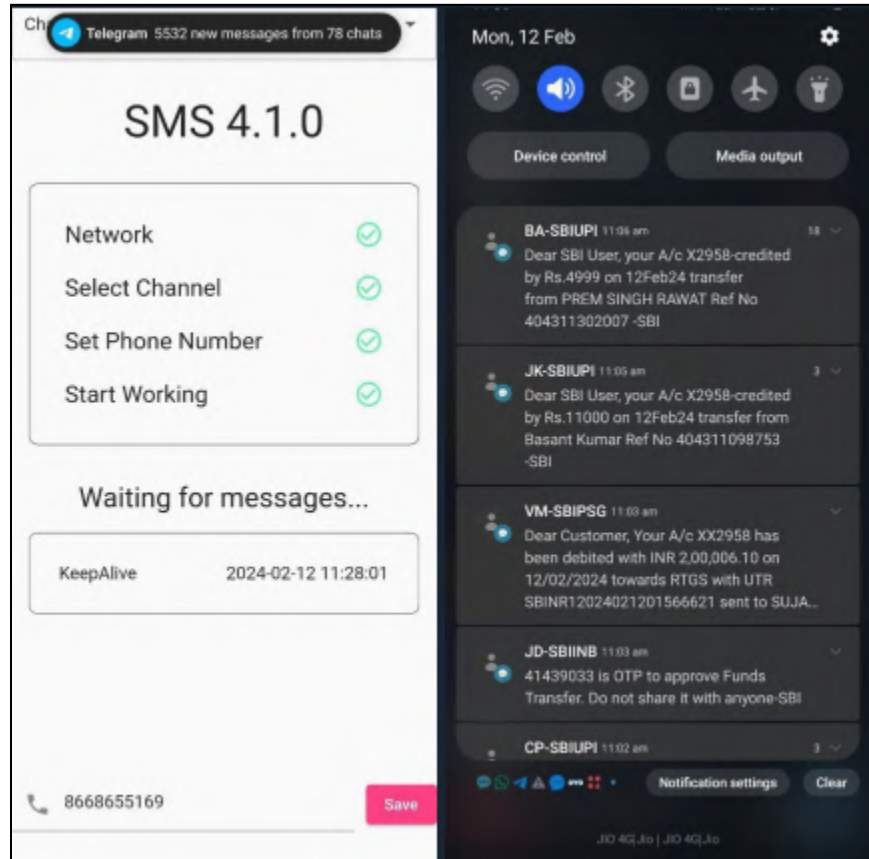
6. Explore Payment Delays for High-Risk Users:

- Investigate the feasibility of introducing short payment delays for identified high-risk users.
- Utilize this "cooling-off" period for further verification and potential intervention before funds are transferred.
- Carefully consider the potential impact on legitimate transactions and user experience before implementation.

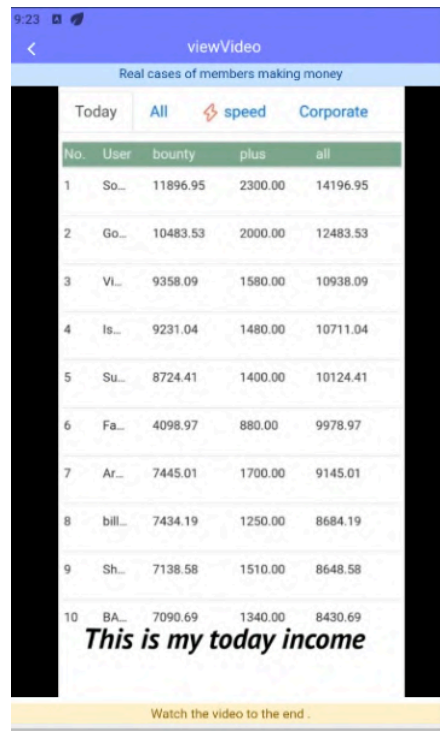
Appendix

2023-11-17 09:54:25	24716	700	Card number:955[REDACTED] Account name: Khir[REDACTED] IFSC:AIRP000[REDACTED] Contact number: 95[REDACTED]	success
2023-11-17 09:53:32	32075	700	Card number:4194[REDACTED] Account name:Sur[REDACTED] IFSC:SBIN000[REDACTED] Contact number: 73[REDACTED]	Audit failure
2023-11-17 09:49:28	31783	43500	Card number:5110[REDACTED] Account name: L[REDACTED] IFSC:SBIN003[REDACTED] Contact number: 78[REDACTED]	success
2023-11-17 09:49:20	31783	50000	Card number:5110[REDACTED] Account name: L[REDACTED] IFSC:SBIN003[REDACTED] Contact number: 78[REDACTED]	success
2023-11-17 09:48:12	33729	420	Card number:1306104[REDACTED] 6 Account name: Dee[REDACTED] IFSC:IBKL000130[REDACTED] Contact number: 9997[REDACTED]	success
2023-11-17 09:43:28	33756	350	Card number:91955[REDACTED] Account name:Jhasal[REDACTED] IFSC:PYTM012[REDACTED] Contact number: 9[REDACTED]	success

App owners posting daily transactions



SMS forwarder used by Agents to forward incoming SMS from mules



Mule mules showing off their incomes to attract more mules

结算日期	通道ID	入账/RS	点位	结算	U价	U数
settlement date	channel ID	into the account	point	settlement	usdt price	quantity
2024.02.12	RB	3180054		73141.2	95	769.9
2024.02.12	RBI	4112205		94580.7	95	995.6
2024.02.12	RBI	2946131		58922.6	93	633.6
2024.02.12	RBI	3698132		77660.8	95	817.5
2024.02.12	SBI	7031822		161731.9	95	1702.4
2024.02.12	SBI	8149197		187443.0	95	1973.1
2024.02.12	SBI	7281968		145639.4	95	1533.0
2024.02.12	SBI	9018110		180362.2	95	1898.5
2024.02.12	SBI	8616528		189563.6	95	1995.4
2024.02.12	IDFC	3891831		89512.1	95	942.2

Mule application owners keeping track of the Transaction Flow



Mules using fake sims to register corporate accounts



Initial Attack Vector Protection Platform

Founded in
2015

200+
CloudSters

3 Offices
HQ: **Singapore,**
Offices:
Bangalore, India
London, UK

200+
Clients Globally

4
Products

We secure some of the Fortune 500 and Unicorns



... And we are backed by eminent investors



Accelerated by



NETAPP
EXCELLERATOR

CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services. We have been featured in several Gartner market guides and are a **qualified AWS partner**. We are the **Highest Rated Security Threat Intelligence company** on Gartner Peer Insights from the Asia Pacific region.



About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.



www.cloudsek.com
info@cloudsek.com