



Chinese Dark Web Syndicates and the Global Money Mule Pipeline to Indian Banks

Category

Adversary Intelligence

Region

Global



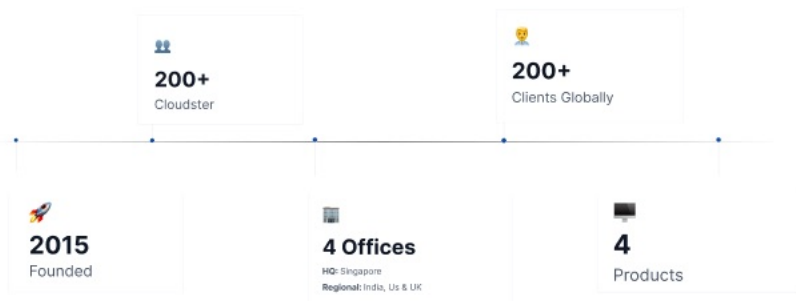
Mayank Sahariya
Cyber Threat Analyst

Passionate about national security and dedicated to advancing capabilities in cyber threat intelligence, the author specializes in investigating organized cybercrime, conducting in-depth malware analysis, and navigating darkweb ecosystems. With a keen focus on the intersection of cybersecurity and financial technology, his work supports law enforcement, intelligence communities, and fintech sectors in identifying and mitigating emerging threats.

Table of Contents	Page No.
1. Executive Summary	03
2. Introduction	04
3. The primary clients of these Illegal Payment Gateways are	04-05
4. The Anatomy of the Operation: A Step-by-Step Breakdown	05-12
5. The Money Laundering and Fraud Cycle: From Deposit to Exfiltration	13-22
6. Statistics from “Mule as a Service”	22-25
7. Real-World Case Studies (Based on Law Enforcement Actions)	25
8. Impact and Threats	25-26
9. Recommendations and Countermeasures	26-27
10. Conclusion	27
11. Appendix	27-29

About CloudSEK

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.



... And we are backed by eminent investors



'Customer First' certified on Gartner Peer Insights

4.8 ★★★★★

Ranked No.3 in the World

Ranked No. 1 in APAC



Executive Summary

This report details the sophisticated and pervasive operations of Chinese-led syndicates that have established a parallel, illegal payment gateway (Payment Gateway) system by systematically exploiting India's digital banking infrastructure. These Payment Gateways function as the financial backbone for a massive, multi-million dollar shadow economy, primarily facilitating money laundering for illegal online gambling, fraudulent investment schemes, and predatory lending applications.

The core of this operation is the large-scale harvesting of Indian "mule" bank accounts—including savings, current, and corporate accounts. These accounts are acquired through a multi-pronged recruitment strategy that targets vulnerable Indian citizens via fraudulent apps, face-to-face agents, and "work-from-home" OTP-sharing scams.

Once controlled, these accounts are integrated into a technically complex dashboard. This allows the syndicates to offer "payment solutions" to their illicit clients (e.g., gambling websites), routing tainted money through a complex web of layers to obscure its origin. The final stage involves exfiltrating the laundered funds out of India, typically through cryptocurrency (USDT-Tether) or hawala networks.

This shadow banking system poses a significant threat to India's economic sovereignty, national security, and the integrity of its financial systems. It facilitates a massive drain of capital, evades taxation, victimizes countless citizens, and undermines regulatory control. Combating this threat requires a coordinated, multi-stakeholder approach involving financial institutions, regulators, law enforcement, and a concerted public awareness effort.

Introduction

The rapid digitization of India's economy, spearheaded by the Unified Payments Interface (UPI), has created unprecedented convenience but has also opened new avenues for financial crime. Transnational criminal organizations, primarily operating from the Mekong region and Southeast Asia, have capitalized on this digital ecosystem to build clandestine financial networks.

These networks function as Illegal Payment Gateways. Unlike legitimate payment gateways (like Razorpay or PayU) that are regulated by the Reserve Bank of India (RBI), these Payment Gateways operate entirely in the shadows. They provide the critical service of moving money for criminal enterprises that cannot access the formal banking system.

The primary clients of these Illegal Payment Gateways are:

1. Illegal Gambling and Betting Platforms:

Including online casinos, slot machine apps, and popular "crash games" like Aviator that are often hosted offshore and promoted through Telegram, social media, or clone app stores.

2. Ponzi and Investment Schemes:

Apps and websites promising unrealistic high returns, often operating without regulatory oversight, lure users into fraudulent schemes.

3. Predatory Digital Lending Apps:

Unregulated apps charge excessive interest, collect personal data without consent, and use harassment or blackmail for debt recovery.

4. Digital Arrest Scams:

Fraudsters impersonate law enforcement or government officials, claiming the victim is under investigation and must pay "penalty" amounts to avoid arrest, often demanding payments through illegal gateways.

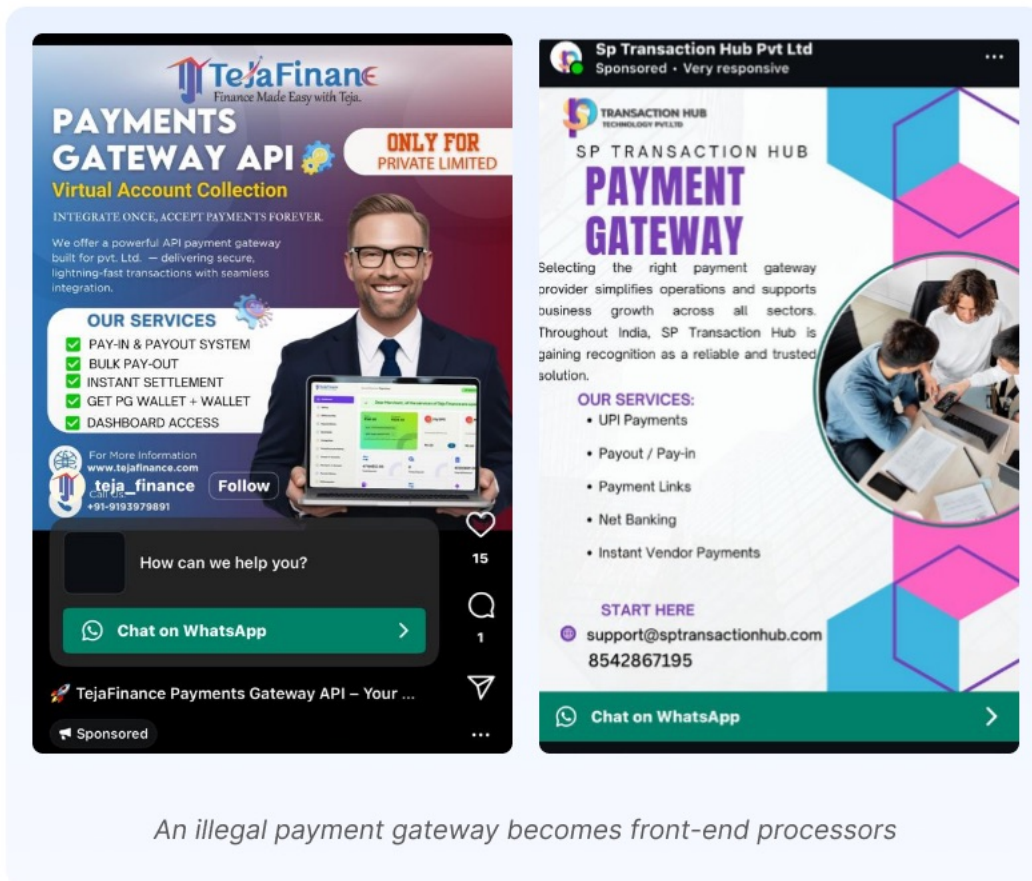
5. Fake Stock Trading Platforms:

Scam trading apps and websites that simulate profits to convince users to deposit more funds, then freeze withdrawals or vanish, leaving victims with significant losses.

6. Illegal Fintech Service Platforms:

A growing number of shell companies have acquired access to Chinese online payment gateway APIs, positioning themselves as legitimate payment service providers. These entities act as front-end processors, offering payment solutions to both legitimate businesses and illicit operators, including:

- Illegal gambling and betting platforms
- Investment fraud schemes and Ponzi apps
- Unlicensed forex/trading websites



By masquerading as fintech or e-commerce solution providers, these shell companies create a veneer of legitimacy around their operations.

To enhance this facade, they engage in online whitewashing tactics, including:

- Paid advertising on Google, Facebook, Instagram, and YouTube
- Creating polished websites and dashboards to mimic real gateway providers
- Publishing fake client testimonials and PR articles
- Using SEO to suppress negative mentions or blacklist alerts

The Anatomy of the Operation: A Step-by-Step Breakdown

The operation can be understood as a sophisticated supply chain with distinct, yet interconnected, stages.

Stage 1: The Recruitment of Mule Accounts

The foundation of the entire Payment Gateway system is a vast pool of Indian bank accounts. The syndicates employ a variety of methods to acquire these accounts.

App-Based Recruitment

Multiple mobile applications are being distributed through **unverified sources** on **Telegram channels and groups**, primarily targeting individuals to **harvest mule accounts**. These apps typically request **sensitive banking information**—such as UPI IDs, account numbers, and login credentials—and gain access to **OTP messages** by abusing device permissions during installation.

Once installed, the apps operate in the background to intercept OTPs and facilitate unauthorized transactions, effectively turning the user's account into a **mule for laundering illicit funds**.

We have detailed the app-based recruiting and functioning in a previous whitepaper that can be accessed [here](#)

Big Winner	Xhelper	Jeevan	Earnbox	Petross	Xwallet	Honeygain	FirePay
Xinpay	Yoloearn	Seepay	KuveraPay	MagicPay	Sarkpay	Toppay	Earnpay
	SafePay	Spro Deal	ShowPay	Lakshmi	Bitearn	Zpay	

List of Applications that are used to manage and oversee mule operations created by Threat Actors

These apps are often disguised as **earning platforms, wallets, or investment tools**, but in reality, they serve as **entry points for large-scale financial fraud and money laundering operations**.

Mechanism:

Fraudulent apps are circulated via closed Telegram or WhatsApp groups. Upon installation, these APKs request extensive permissions—especially access to SMS messages—allowing them to intercept One-Time Passwords (OTPs).

Modus Operandi:

- Users are lured with offers to earn 2–3% commission on transaction volumes.
- They are asked to submit sensitive banking details such as **UPI IDs** or **Merchant QR codes**.
- The app silently captures OTPs and authentication data in the background.

Outcome:

The syndicate gains full or partial control over the victim's bank account, either by directly harvesting credentials or intercepting OTPs to authorize unauthorized transactions.

Face-to-Face Recruitment (On-the-Ground Agents)

Mechanism:

Local Indian agents, often recruited through Telegram or WhatsApp groups, are paid commissions to open new bank accounts.

The Target:

They target vulnerable individuals: unemployed youth, students, laborers, and people in rural areas with low financial literacy.

The Process:

- The agent offers a lump-sum payment (e.g., ₹10,000 - ₹20,000) on saving accounts to 1-5 crores to a corporate account, depending on the transaction limit of the account or a monthly commission for "renting" the bank account.
- The victim is persuaded to open a new Savings or Current Account.
- The agent takes the debit card, cheque book, and the SIM card linked to the account. This gives them complete control over OTPs and transactions.
- For Corporate Accounts, the process is more sophisticated. Agents create shell companies using [forged](#) or stolen identity documents (PAN, Aadhaar) of complicit or unwitting individuals. These corporate accounts are highly prized as they can handle larger transaction volumes and appear more legitimate, thus avoiding initial red flags.

"OTP Work" and Task based Scams

Mechanism:

A newer, more insidious method advertised as a "work-from-home" job.

The Task:

The "job" is simply to receive OTPs on a designated SIM card and forward them to a handler in real-time. OTP work requires a security deposit from the mule side, ensuring they don't go away after receiving funds.

The Reality:

The individual is acting as a human OTP relay for fraudulent transactions being conducted by the syndicate on a mule account they control. This provides a layer of deniability for the operators.

Gabrielle Ryan Catie
Sponsored

Renting company account –

Axis – IOB

IBKL

Yes.

'bandhan

KARB/AU

IDFC

RBL

Apply now

Join India's leading payment company! Start earning money now! Enjoy our secure and stable platform! If you are an Indian business owner with a business account, Apply now for details

Good news!!!

We are a large, reputable and well-known payment company. We are looking for strong Indian partners to provide us with daily corporate account services. We offer high transaction volume and very competitive commission rates (all commissions are within the framework of safe and compliant game funds) (account holders need to come to our company for face-to-face transactions) (savings accounts and current accounts are not accepted)

Supported Banks:

Bandhan Corporate (₹1-5 Cr Limit)

AU Corporate (₹1-5 Cr Limit)

IDFC Corporate (₹1-5 Cr Limit)

IDBI Corporate (₹1-5 Cr Limit)

BOM Corporate & Current

No job consultation! (We do not provide any job opportunities)

Our company only cooperates with capable people to do business!!!

APPLY NOW

Rent bank accounts for game fund for earning 1-3 Lac in 7 days.

If you have bank accounts under business name like Proprietaryship or Private Company, not under personal name, and has MQR(Merchant QR) or has bulk mode enabled, contact us.

Especially need these now:

Need with MQR: BOM(Bank of Maharashtra),Suryoday,SBI CMP,SBI with e-service,SBI 3 login ID,SBI 4 login ID,RBL, Canara corporate/retail with MQR,TMB(Tamilnad Mercantile Bank),CUB(CITY UNION BANK),HDFC 2id,J&K Bank),Equitas Bank corporate

Need with Bulk mode: Axis paypro with IMPS,yesbank with bulk,idfc with bulk

Contact us for your accounts

Big win Brazil

Learn more

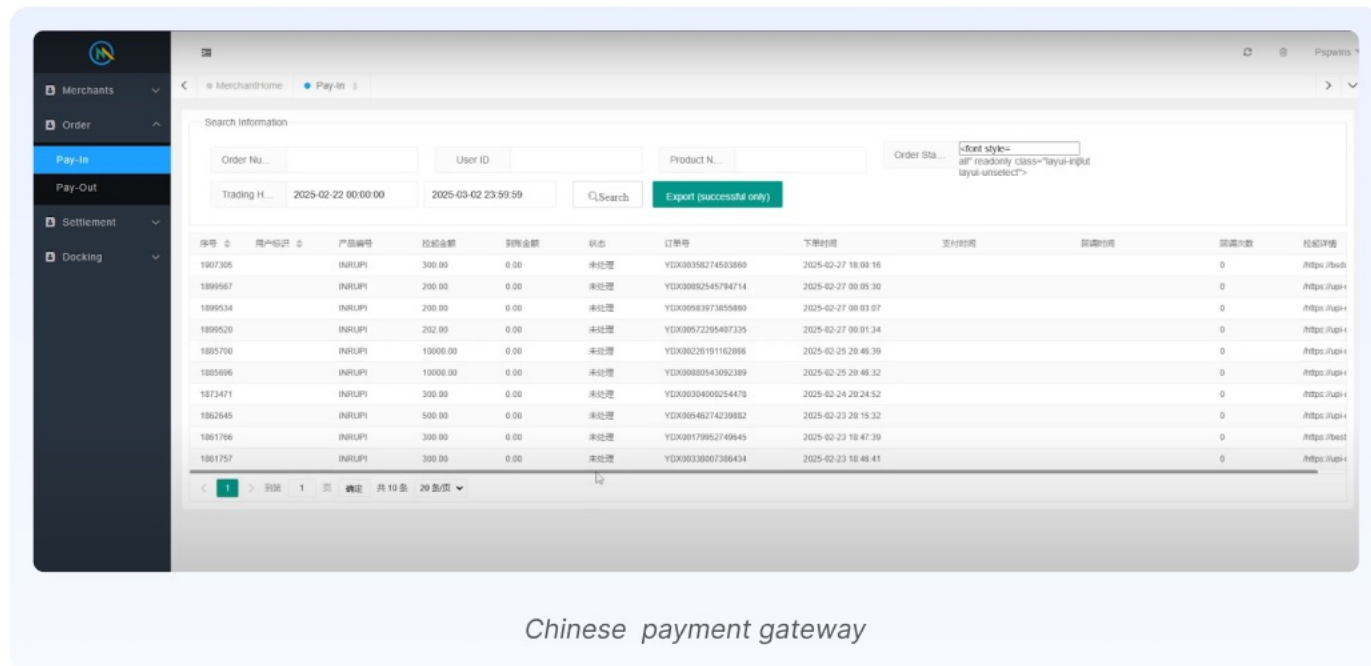
Stage 2: Technical Integration and Gateway Creation

Once the accounts are harvested, they are integrated into a centralized technical infrastructure, effectively creating a payment gateway.

Chinese operators utilize a custom-developed software dashboard to control their operations. They integrate thousands of mule accounts into this system using API credentials or App based access and net banking information. Through the bulk payout feature of current and corporate accounts, they execute large volumes of transactions via payment gateways efficiently.

There are over **100 Telegram channels** actively engaged in either **collecting bank accounts for mule use** or **offering illegal payment gateway services**. The following payment gateway providers have been identified as **actively supporting illicit financial activities**, including **money laundering, fraudulent app monetization, illegal gambling, and Ponzi schemes**. These gateways are often integrated into scam ecosystems and offer **non-compliant APIs, crypto cashouts, and dynamic UPI routing**:

Bsdpay	Cecopay	Dragonpay	Gtrpay	Holipay	Ipay	Iqpay	Jdpay	Lpay
Magicpay	Superpay	Worldpay	Luckypay	Arpay	Skpay	Spokpay	Wepay	
Pengupay	Richpay	Rubypay	Sunpay	Wkpay	Hefupay	Hefupay	Haoxpay	
Horsepay	Okpay	Funpay	Wow pay	Ospay	Gaaypay	Cpupay	Wddpay	
				Hisoapay				



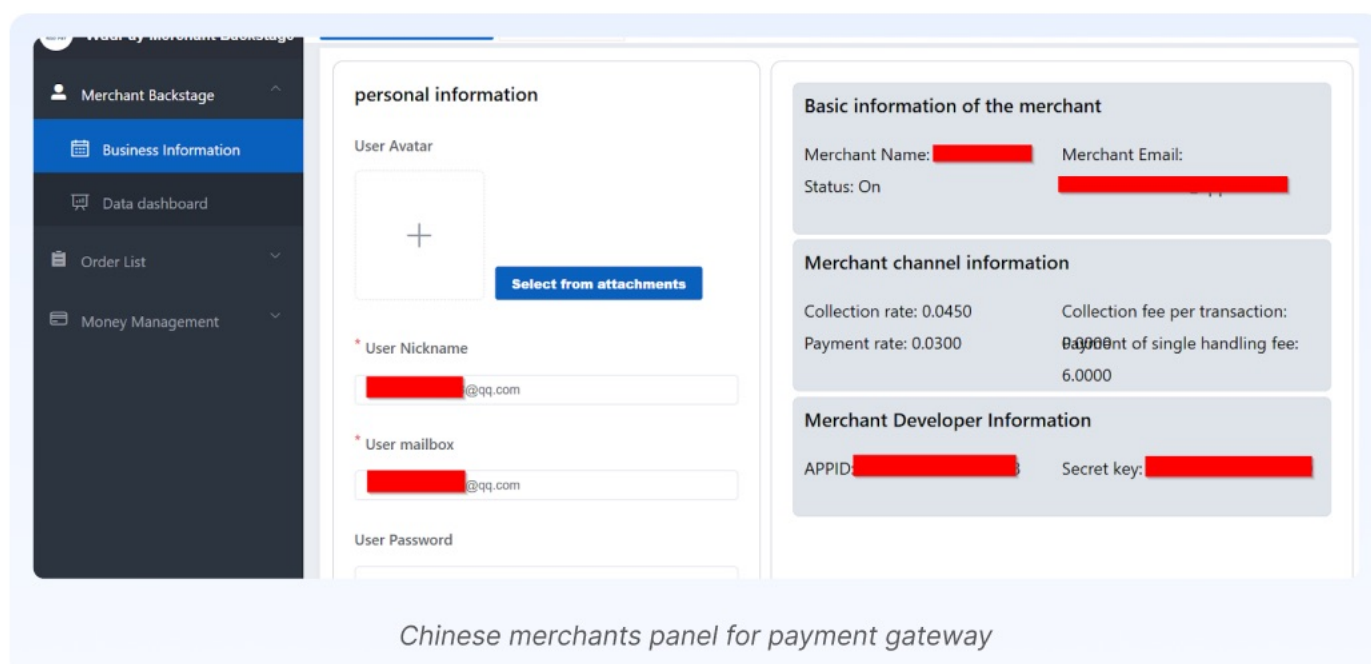
Chinese payment gateway

Integration with Scam Platforms:

The gateway provides API keys (AppID & Secret Key) that can be easily integrated into **fraudulent apps** such as Ponzi schemes, fake investment portals, illegal online casinos, and betting platforms.

The screenshot below reveals merchant developer credentials—specifically, the AppID and Secret Key—provided by a Chinese payment gateway. These credentials can be easily misused by Ponzi schemes, fraudulent gambling apps, and illegal casino platforms to integrate the gateway and facilitate large-scale money laundering through API-based transactions.

The merchant channel details indicate that the payment gateway charges a **4.5% fee on Paying (collection) transactions** and a **3% fee on each Payout transaction**.

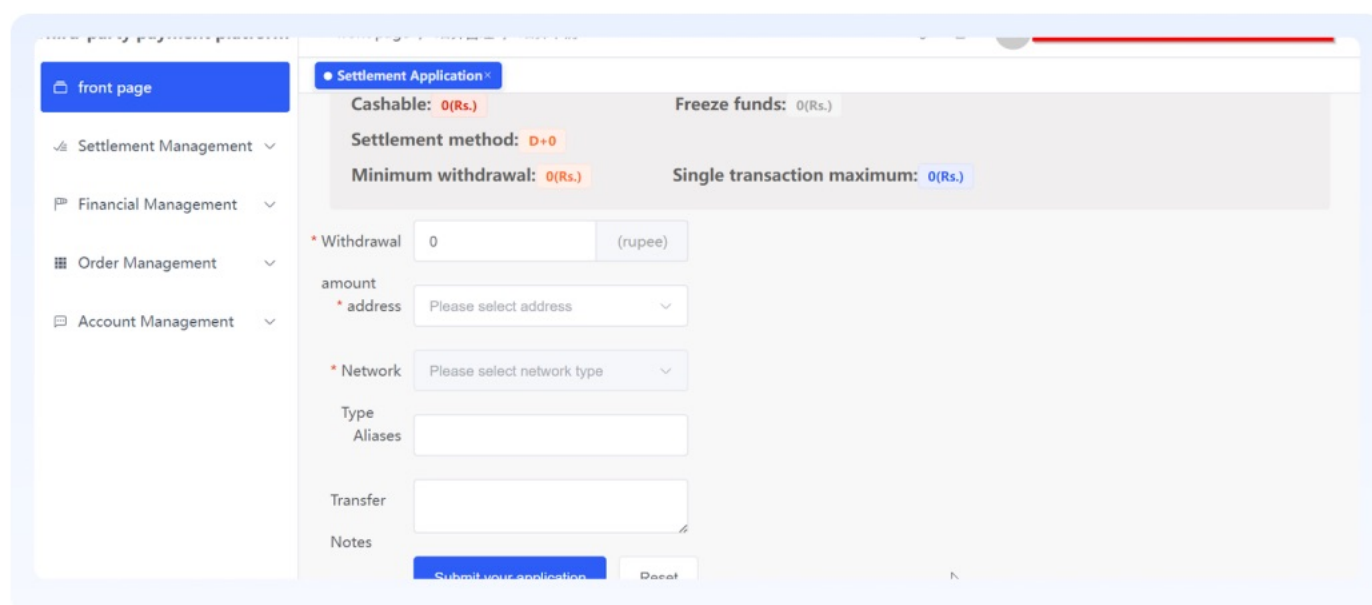


Chinese merchants panel for payment gateway

In another payment gateway instance, the dashboard interface displays modules such as **Settlement Management**, **Financial Management**, **Order Management**, and **Account Management**. These features enable illicit clients to efficiently **monitor, control, and manipulate the overall transaction flow**, supporting fraudulent operations at scale.



Several non-compliant Chinese-origin payment gateway providers offer **crypto cashout services** to support the illicit financial ecosystem. These services play a critical role in helping scam operators obscure the source of their illicit funds and bypass regulatory scrutiny.



API for Illicit Clients: The gambling or Ponzi scheme website integrates a simple API provided by the Payment Gateway operator. When a user in India clicks "Deposit," Payment Gateway's system automatically assigns one of the available mule account's merchant QR code to receive the payment.

Global Description
Signature Verification
Collection
Collect asynchronous callbacks
Create a collection order POST
Check collection order GET
Payment
Payment asynchronous callback
Create a payment order POST
Check payment order GET
UTR order POST
Check balance GET

- https://api. [REDACTED]
- Interface domain name + request url = final interface request address

Order status (collection, payment)

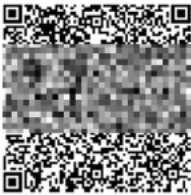
- Order Status (orderStatus): 1-pending, 2-pending payment, 3-paid, 4-payment failed, 5-cancelled payment

Request result return description


```
code = 10000代表成功, 其他值 代表失败
{
  "code": 10000,
  "message": "success",
  "data": {
    "appId": "814cdfc2c697485XXXXXXXXXX",
    "platformOrderNumber": "test654321",
    "orderNumber": "test123456",
    "amount": "100",
    "feeRate": "0.2000",
    "fee": "100.6000",
    "realAmount": "100.4000",
  }
}
```

Account Rotation: The system is programmed to rapidly rotate the receiving Merchant QR accounts. An account might only be used for a few transactions or for a limited time (a few hours) before being replaced to avoid being flagged by a bank's anti-money laundering system.

Total Amount Payable: ₹ 500.00

SCAN & PAY


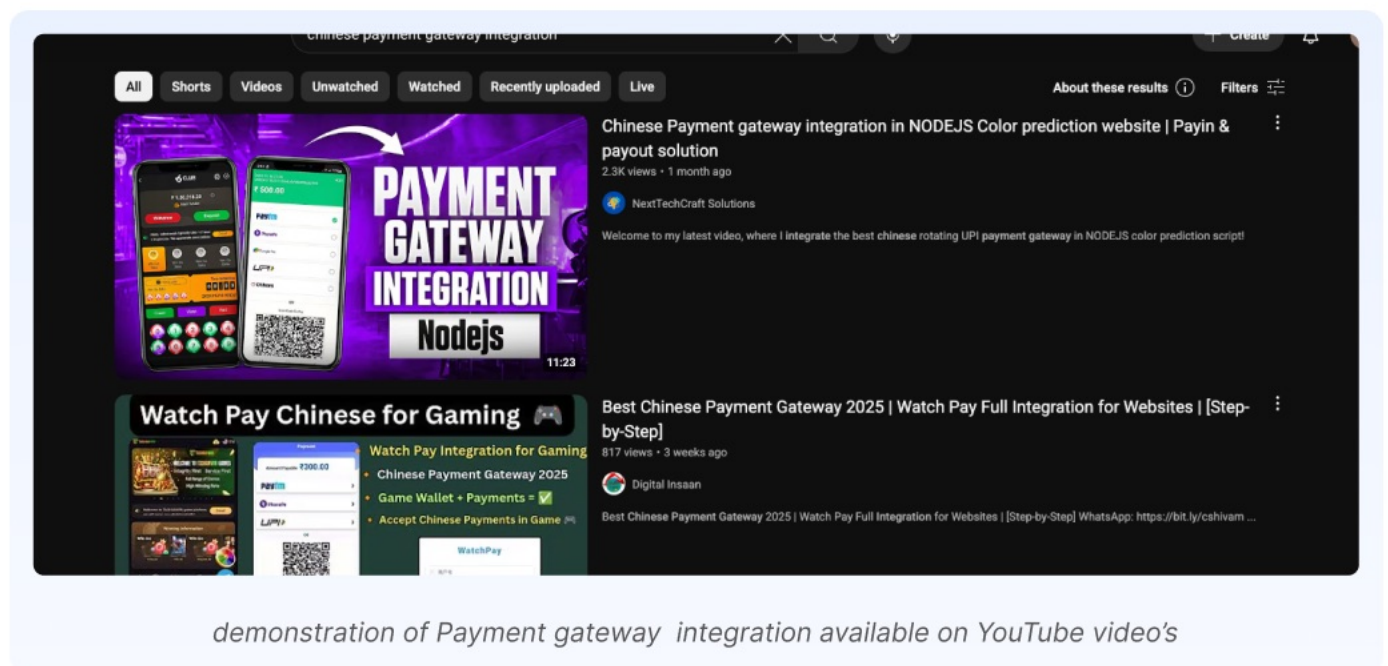
elect a payment method to Pay


Best speed to credited amount

YouTube Becomes a Training Ground for Illicit Payment Gateway Integration

Operators of **fraudulent apps** and **illicit platforms** using **Chinese-origin payment gateways** are increasingly seeking **YouTube video tutorials** to assist with the **integration process**. Commonly showcase:

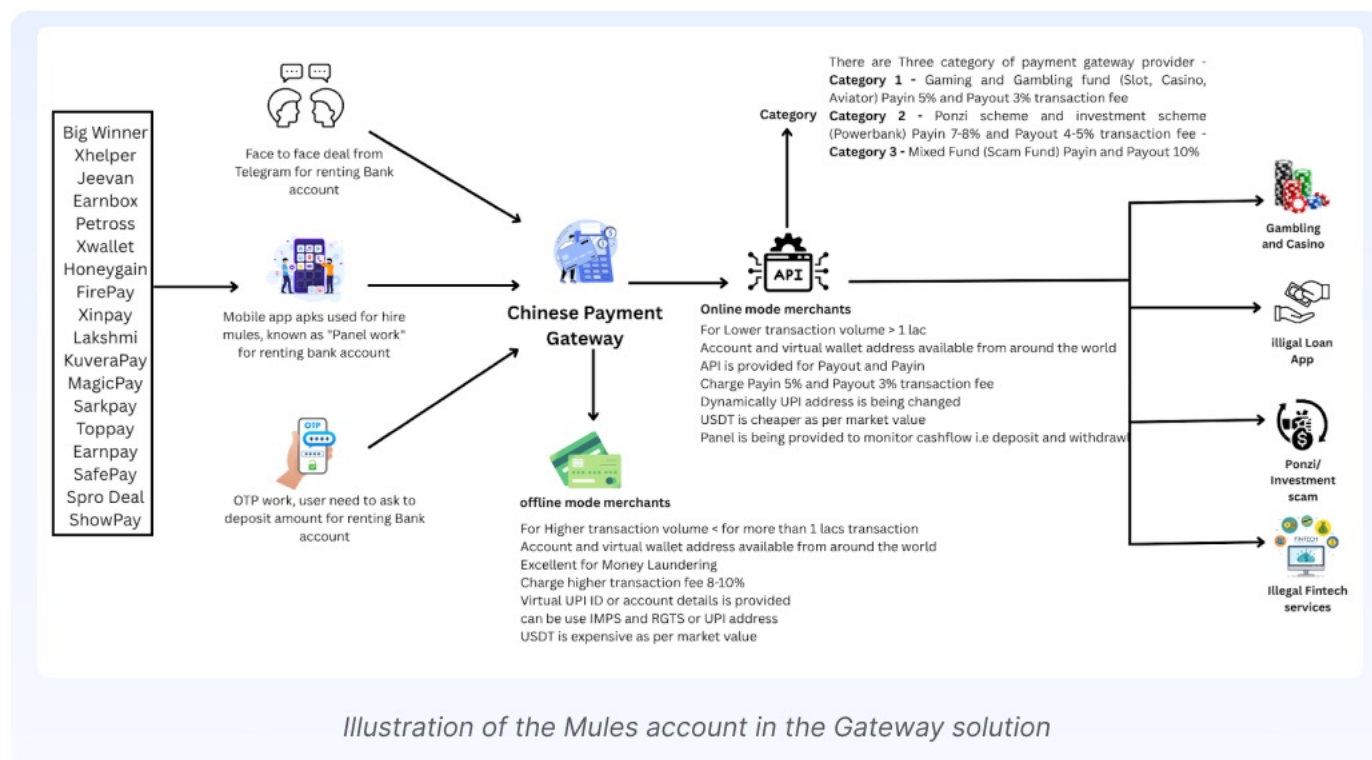
- How to implement **API keys** (AppID and Secret Key)
- Step-by-step **integration with scam platforms** (e.g., gambling, fake investment, or loan apps)
- How to automate **Pay-in and Payout flows**
- Usage of **merchant dashboards** and **crypto cashout features**



demonstration of Payment gateway integration available on YouTube video's

These tutorials serve as **onboarding aids** for non-technical operators, allowing even low-skilled fraud actors to set up **fully functional laundering systems** using the gateway infrastructure. A small portion of active instructional videos have collectively garnered over **37,200 views**, indicating a significant level of interest and usage. Refer to the [Appendix](#) for a list of non-exhaustive channels and videos

The Money Laundering and Fraud Cycle: From Deposit to Exfiltration



Comparison table between Offline Merchant Gateway and Online Merchant Gateway,

Criteria	Offline Merchant Gateway	Online Merchant Gateway
Transaction Volume	Higher (More than ₹1 lakh)	Lower (Less than ₹1 lakh)
Account/Wallet Availability	Global account and virtual wallet address available	Global account and virtual wallet address available
Usage Intent	Excellent for Money Laundering	Mostly for small, scattered financial movements
Transaction Fee	8-10%	5% for Payin, 3% for Payout
UPI/Account Details	Static or virtual UPI/account details provided	Dynamic UPI address (changes regularly)
Banking Methods Supported	IMPS, RTGS, UPI	UPI (primarily), some support IMPS
USDT (Tether) Usage	Expensive (higher than market rate)	Cheaper (lower than market rate)

Criteria	Offline Merchant Gateway	Online Merchant Gateway
Monitoring Panel	No monitoring tools	Dedicated dashboard for deposit and withdrawal monitoring
API Support	Not available	API provided for both Payout and Payin
Withdrawal	USDT only	USDT and Bank Account

Online Merchant Gateway:

Online Merchant Gateways are digital platforms that allow merchants to collect payments from customers through various online channels—primarily UPI, virtual accounts, or card payments. While these platforms are essential for legitimate e-commerce operations, non-compliant or rogue versions are increasingly being used by fraudsters, scam apps, and illicit financial networks to move and clean money under the radar.

Classification of Payment Gateway Providers Based on Client Use Cases

Illicit payment gateway providers are typically segmented into three categories based on the **nature of the clients they serve** and the **risk profile of the transaction funds**. Each category has **different transaction fee structures** to reflect the associated legal and reputational risks.

Category 1: Gaming & Gambling Funds

Client Type:

Online casinos, slot machine apps, crash games like Aviator, and illegal betting platforms.

Use Case:

High-volume daily transactions with rapid Payin and Payout cycles.

Fees:

Payin – 5%, Payout – 3%

Risk Level:

Medium

While illegal in many jurisdictions, these platforms often operate under offshore licenses or disguised app formats.

Category 2: Ponzi & Investment Schemes

Client Type:

Fake investment apps, "power bank" schemes, high-return platforms, and fraudulent financial products.

Use Case:

Collecting large volumes from unsuspecting investors with little to no withdrawal activity.

Fees:

Paying – 7–8%, Payout – 4–5%

Risk Level:

High

These schemes often collapse, attracting regulatory attention and financial fraud investigations.

Category 3: Mixed or Scam Funds

Client Type:

Platforms engaged in multiple fraud types—loan scams, phishing, fake e-commerce, crypto doubling, and more.

Use Case:

Heavily abused for laundering multi-source scam funds, often with volatile transaction flows and multiple layers of mule accounts.

Fees:

Paying – 7–8%, Payout – 4–5%

Risk Level:

Critical

Considered the highest-risk category, these gateways are frequently associated with **organized cybercrime** and **cross-border laundering networks**.

Below are the key features & functionality of this payment gateway:

Dynamic UPI Infrastructure:

- These gateways generate **dynamic UPI IDs** or QR codes for each transaction, making it difficult for financial institutions to detect patterns or flag repeated misuse.
- Since each payment link or address expires quickly, this reduces the risk of blacklisting or traceability.

API Integration:

- Full **API support** is available for both **Payin (collection)** and **Payout (withdrawal)** operations.
- This allows scammers to **automate fund collection**, control transaction flows in real-time, and **integrate directly into scam apps** (e.g., fake trading platforms, gambling apps, etc.).

Global Wallet & Account Access:

- Many such gateways offer **global virtual accounts and wallets**, enabling users to receive payments in multiple currencies, then convert them into **crypto assets like USDT** or transfer across borders easily.

Dashboard & Monitoring Tools:

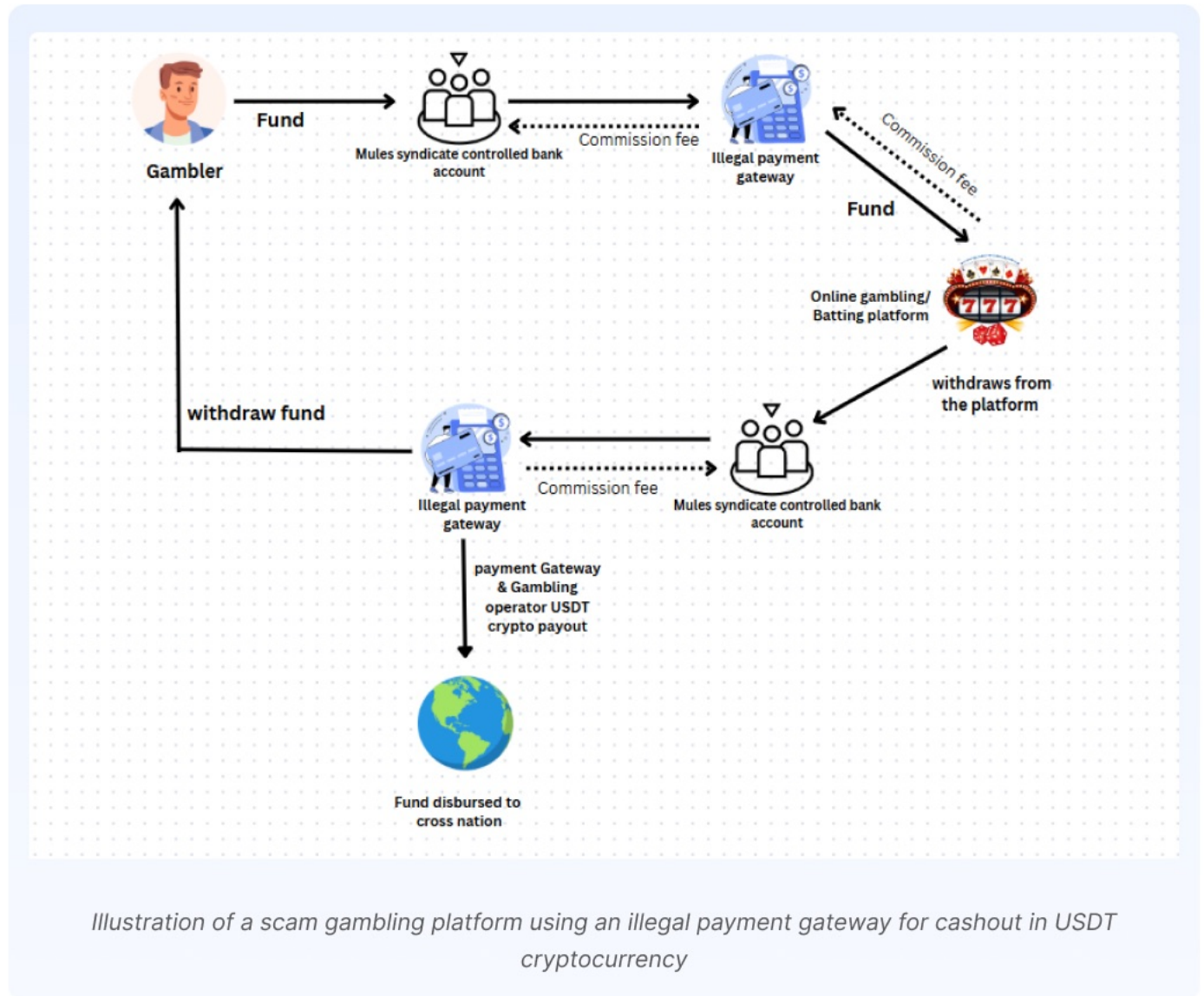
- Operators are provided with a **web-based admin panel** to manage deposits, withdrawals, user activity, and account balances.
- This visibility makes it convenient to **track money movement**, assign funds to downstream accounts, and control flow across multiple mules or merchant fronts.

Moderate Transaction Fees:

- Typically, the gateway charges **5% for Payins** and **3% for Payouts**, which is lower than offline laundering channels and more suitable for **low-value, high-frequency transactions**.

Withdrawal Options:

- Users can **withdraw funds either in USDT or to domestic bank accounts**, depending on the setup and local regulations.
- Crypto cashouts are often handled via OTC (over-the-counter) desks or P2P exchanges integrated with the gateway backend.



The movement of money is meticulously structured to obscure its origin and destination.

Step 1: Collection (First Layer)

- A player on a gambling site deposits ₹5,000.
- The Payment Gateway directs this payment via UPI to Mule Account A (a Savings Account).
- Simultaneously, dozens of other players are depositing funds into Mule Accounts B, C, and D.

Step 2: Layering (Obfuscation)

- Almost instantly, the funds from these primary mule accounts are transferred.
- The ₹5,000 from Account A is moved to Mule Account E (a Current Account), mixed with funds from other accounts.
- This process is repeated multiple times across a web of 7-10 different accounts within minutes.

This rapid, multi-layered movement makes the trail incredibly difficult for bank algorithms and human investigators to follow. Corporate accounts are often used in the mid-layers to handle aggregated, larger sums.

Step 3: Consolidation

- After passing through multiple layers, the funds are consolidated into a smaller number of high-value Corporate Mule Accounts. These accounts, registered under fake shell companies, might hold several crores (tens of millions) of rupees.

Step 4: Integration and Exfiltration (Cashing Out)

- The pooled money is now ready to be moved out of India's financial system. The primary methods are:

Step 4: Integration and Exfiltration (Cashing Out)

- The pooled money is now ready to be moved out of India's financial system. The primary methods are:

Cryptocurrency Purchase: The operators use the funds in the final mule accounts to buy stablecoins, primarily Tether (USDT), on Indian crypto exchanges or through peer-to-peer (P2P) networks. The crypto is then transferred to wallets controlled by the syndicate in China or other locations. This is the most common and efficient method.

Hawala Networks: The cash is withdrawn from the mule accounts and handed over to a traditional hawala operator in India, who then arranges for a corresponding payment to be made to the syndicate abroad.

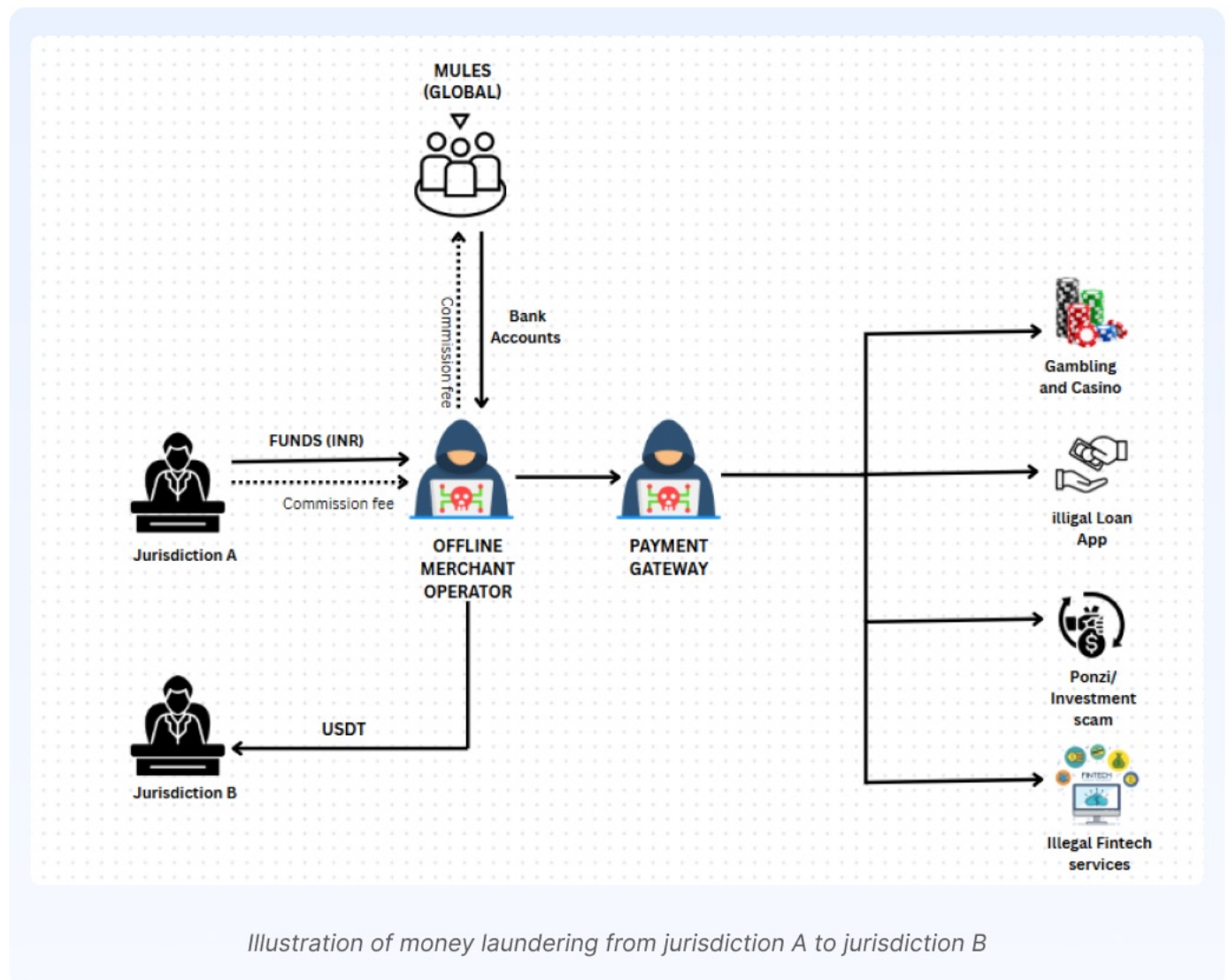
Trade-Based Money Laundering: The shell company associated with the corporate mule account may engage in fake international trade, such as over-invoicing for imported electronics or software from a related entity in China or Hong Kong, thus sending money out through official banking channels under a legitimate pretext.

Offline Merchant Gateway:

Offline Merchant Gateways are a preferred infrastructure for **organized money laundering operations** due to their capacity to handle **high-value transactions** (₹1 lakh and above) and operate outside standard compliance frameworks. These gateways are typically **non-compliant, unregulated**, and often run through shell entities or offshore intermediaries, making enforcement and traceability extremely difficult.

At the core of this laundering mechanism is a **global mule network**. Fraud syndicates **recruit mules across various countries**, including India, Nepal, Bangladesh, Vietnam, Philippines, Pakistan and several African and Eastern European nations. These mules are either:

- **Complicit individuals** who lease or sell their bank accounts, or
- **Unwitting victims** persuaded through job scams, "work-from-home" offers, or small commission-based tasks.



Offline merchant gateways are primarily used for high-volume transactions (₹1 lakh and above) and are favored in large-scale money laundering operations. They provide static or virtual UPI/account details, support IMPS, RTGS, and UPI, and often charge high transaction fees (8–10%). These gateways lack monitoring tools and API support, and withdrawals are typically done via USDT at inflated rates.

The offline merchant gateway service for Mules accounts is sourced from the following countries:



World map showing the presence of the mules account available in the Chinese gateway syndicate

1. Asia & Middle East:

India, Bangladesh, Pakistan, Sri Lanka, Vietnam, Thailand, Indonesia, Philippines, Kyrgyzstan, Uzbekistan, Kazakhstan, Tajikistan, Saudi Arabia, Iraq, Oman, UAE, Lebanon, Singapore, Japan

2. Africa:

South Africa, Kenya, Morocco, Egypt, Nigeria, Ghana, Cameroon, Algeria, Cote d'Ivoire, Angola, Mozambique, Senegal, Guinea, Sudan, Burkina Faso, Tanzania

3. Europe & CIS:

Russia, Ukraine, Belarus, Poland, Germany, Italy

4. Latin America & Caribbean:

Mexico, Brazil, Argentina, Colombia, Uruguay, Dominican Republic, El Salvador

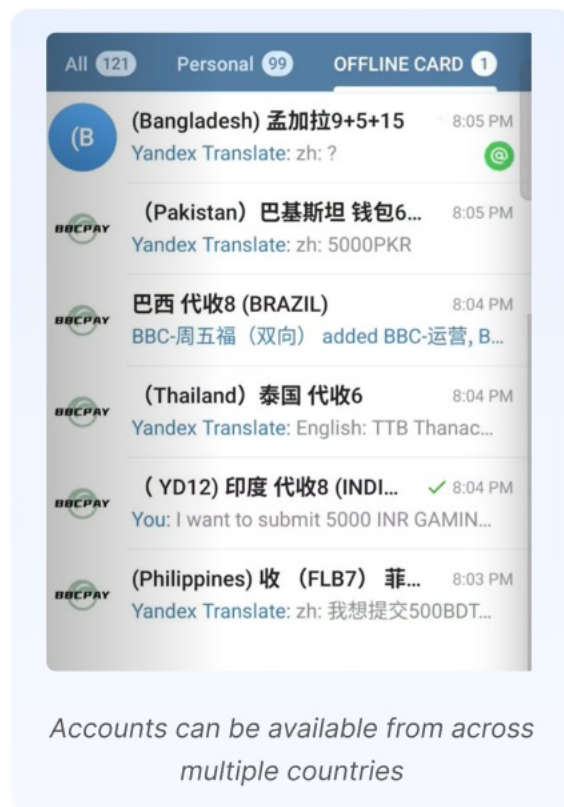
5. Others / International Clusters:

Turkey, Madagascar, International households

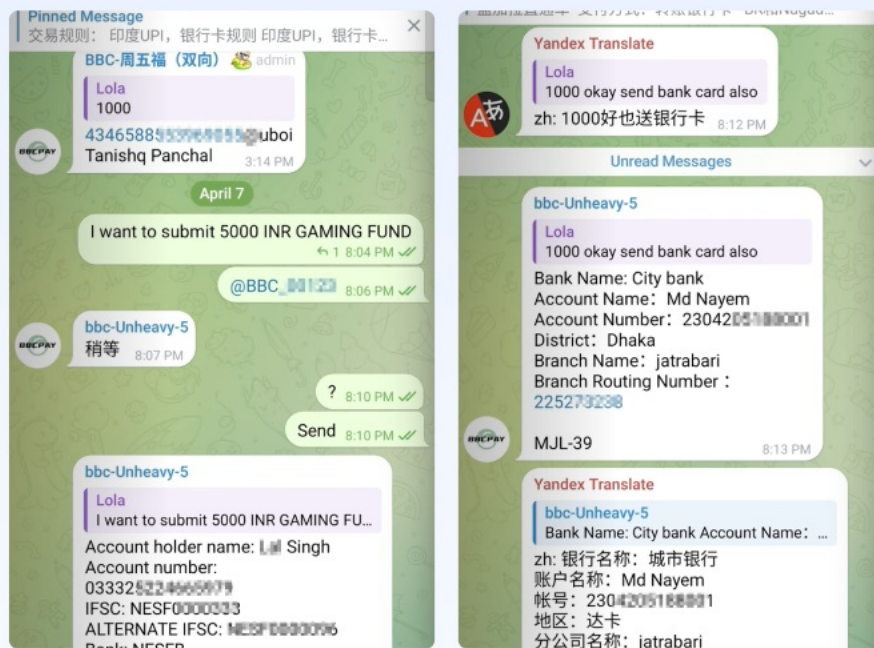


Our investigative team has successfully identified and assessed mule accounts actively being used across a range of high-risk jurisdictions, notably including Pakistan, India, Bangladesh, Brazil, Thailand, and the Philippines.

Upon selecting a specific region, the Offline Merchant Gateway operator assigns the user to a designated regional mule group—typically hosted on Telegram. Within this group, individuals acting as mule account holders from different countries are coordinated to facilitate cross-border fund transfers. The laundering process operates on a trust-based exchange model, where one account holder can send any amount to another mule in a different region. In return, the sender receives the equivalent value in USDT (Tether), either instantly or via a connected P2P crypto vendor. This system bypasses formal banking channels entirely and enables quick, untraceable international money movement.



As part of our investigation, we intentionally joined two region-specific groups—India and Bangladesh—facilitated by the Offline Merchant Gateway operator. These groups function as transaction hubs, where mule account holders from each country are organized and available on-demand for fund movement.



Mule account holders are actively used to enable cash flow movements for money laundering, typically accepting or exchanging funds in return for USDT (Tether).

Statistics from “Mule as a Service”

Our team gained access to a mobile application used to harvest mule accounts, distributed via Telegram and third-party APK sources. It is part of a broader network enabling illicit fund movement and laundering. Since our analysis began, we've reported **~47K mule account activities** across public and private sector banks, linked to transactions worth **₹250 crore**. This includes **around 20.3K unique mule accounts** over several months. Please refer to the [Appendix](#) for a detailed breakdown of the reported mule accounts.

Upon detailed analysis of backend data and transactional records within the app, the following findings were observed:

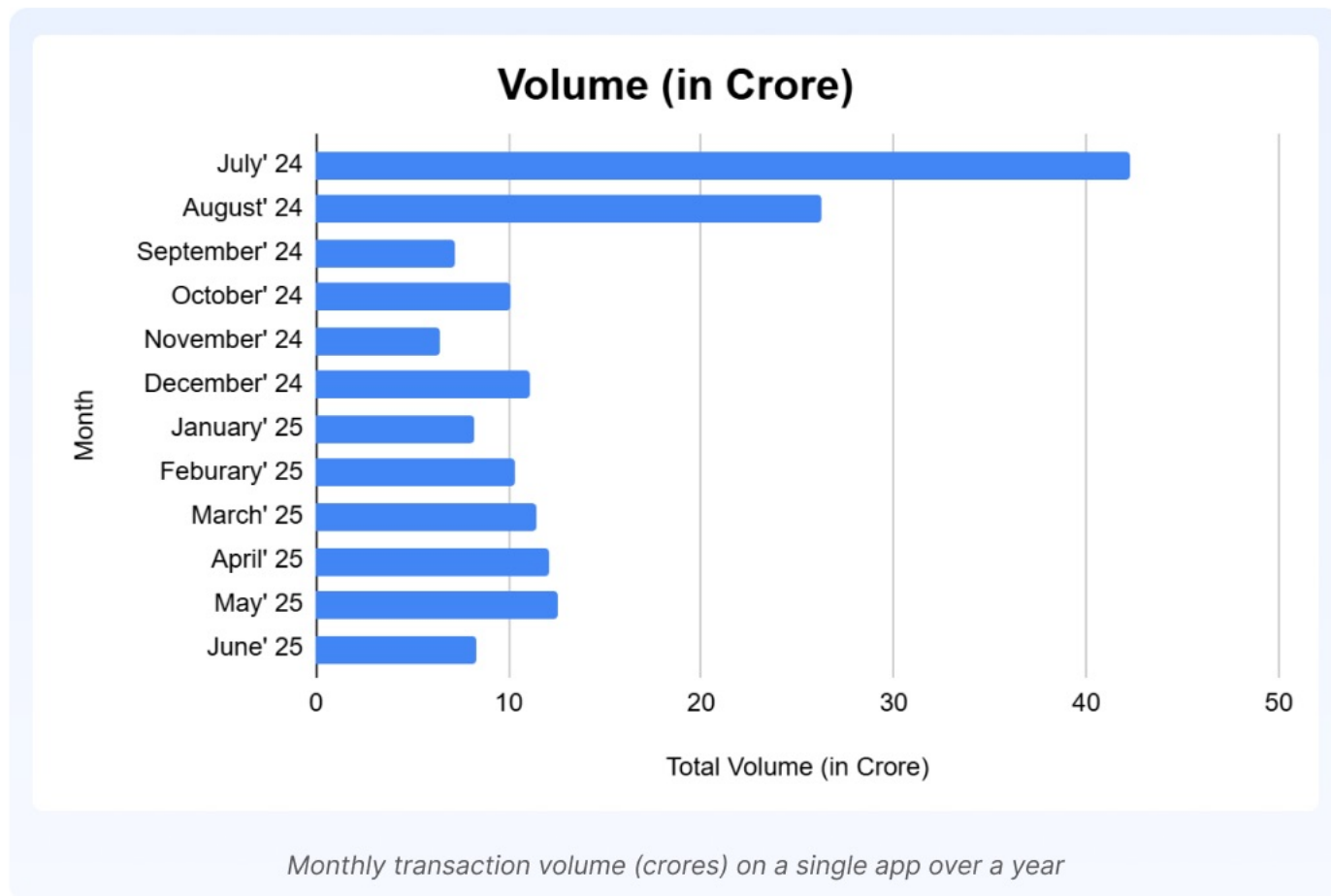
- A staggering **₹166 crore** (INR) in total transaction volume of money
- Spread across approximately **398,675 individual transactions**
- Involving **34,299 mule bank account activities**
- All conducted within a **12-month operational period**
- **20333** Unique mule accounts have been flagged till now

1. Transaction Volume Summary

In a span of 12 months, the identified application facilitated:

- **Total Transaction Volume:** ₹166 crore
- **Monthly Average:** Approx. ₹13.8 crore
- **Daily Flow:** Around ₹45–50 lakh

These funds were routed through mule accounts and likely tied to activities such as **fraudulent lending apps, betting platforms, and Ponzi-style schemes**.



2. Mule Account Exploitation Summary

The app made use of a large and organized mule network:

- **Total Mule Accounts Used:** 34,299 bank/UPI accounts activities
- **Account Types:** Savings, current, and UPI-linked wallets
- **Behavior:** Accounts were either rented, purchased, or accessed via credential harvesting (e.g., OTP theft via APKs)

This scale of mule involvement indicates a **systematic laundering infrastructure**, with decentralized recruitment and distributed fund routing.

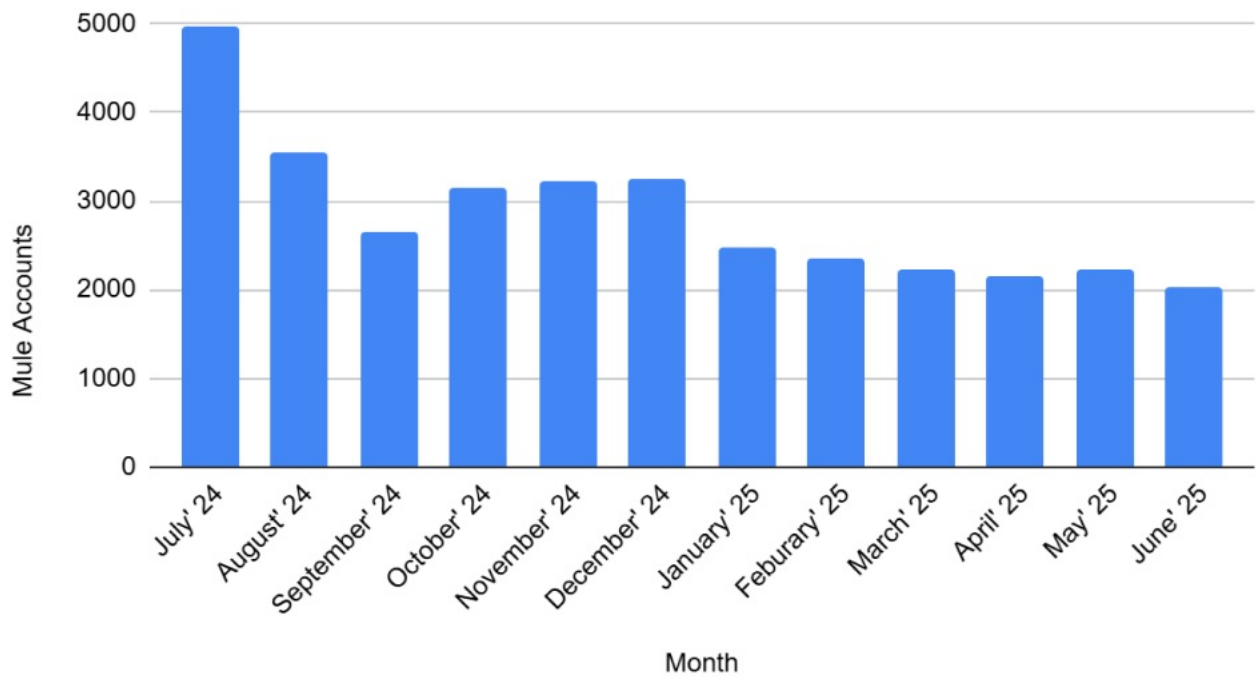
3. Transaction Count Summary

The backend analysis of the application revealed:

- **Total Transactions:** 398,675 individual fund movements
- **Monthly Average:** Over 33,000 transactions
- **Daily Average:** Around 1,100–1,300 transactions

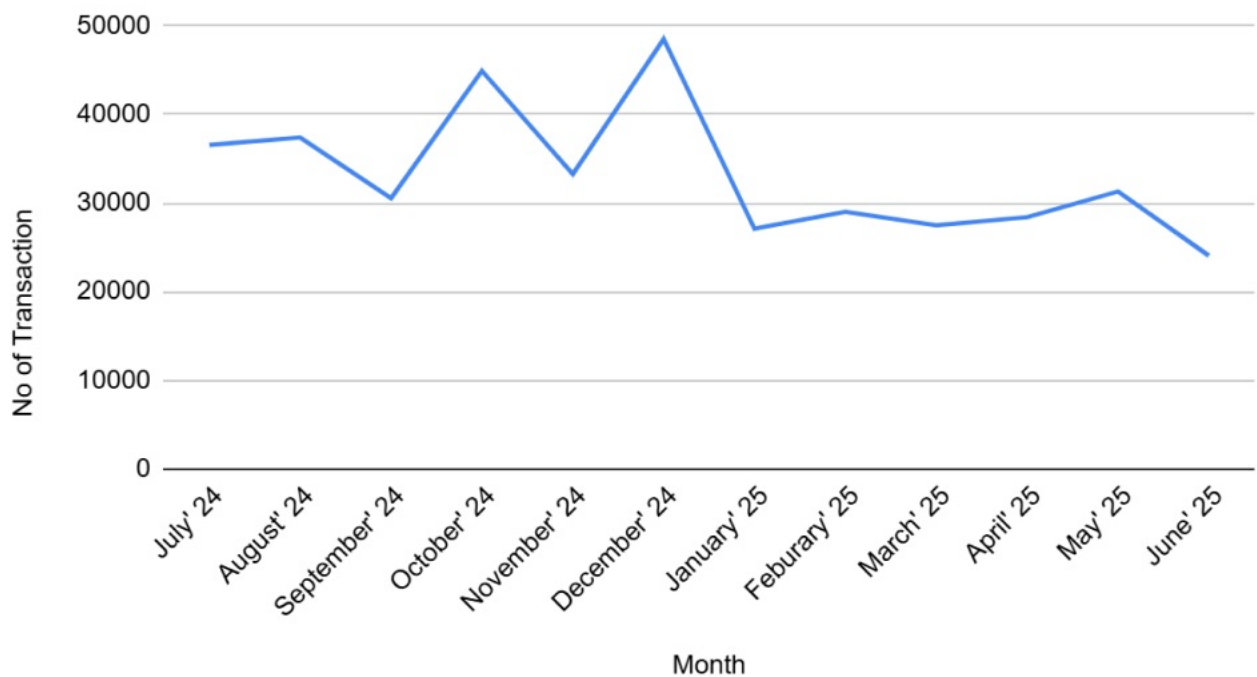
This reflects a **high-volume laundering operation**, with steady inflows and outflows processed through multiple banking channels and payment methods.

Mule Accounts



Monthly mule account on a single app over a year

Transactions



Monthly transactions on a single app over a year

By extrapolating the known figures from the confirmed app to the wider network of **25 similar applications**, the **estimated scale of illicit financial activity** could be:

- **Total Volume Laundered:** ₹4000 crore – ₹5000 crore per year
- **Total Transactions:** 9 – 10 million annually
- **Mule Accounts Exploited:** Over 850,000-900,000 accounts
- **Average Daily Volume Across Ecosystem:** ₹10-15 crore per day

These laundering platforms pose an **urgent and strategic threat** to financial systems, digital regulatory frameworks, and the integrity of payment infrastructure across multiple jurisdictions.

According to the **Indian Cybercrime Coordination Centre (I4C)**, nearly **4,000 mule accounts are being identified daily**, actively used as intermediaries in **money laundering operations**. In response to this growing threat, **I4C has recently issued an [advisory](#)** to raise awareness and guide enforcement and financial institutions on mitigation measures.

Real-World Case Studies (Based on Law Enforcement Actions)

The Hyderabad Police Investigation (2022): Uncovered a ₹700+ crore money laundering operation linked to investment and gambling scams. The investigation revealed Chinese nationals operating from Dubai, using Indian accomplices to set up 61 shell companies and numerous bank accounts to launder funds to China via cryptocurrency.

The Enforcement Directorate (ED) Crackdown (2022-2023): The ED has frozen hundreds of crores of rupees across multiple investigations into predatory loan apps and gambling apps. Their findings consistently point to Chinese-controlled entities using a web of mule accounts and shell firms, with funds being siphoned off via crypto or hawala.

Odisha EOW (Economic Offences Wing) Bust (2023): Revealed a scam where over 1,000 mule accounts were opened by targeting villagers. Scammers paid them a small commission to open accounts and hand over their credentials, which were then used to launder over ₹1,000 crore from various cyber-scams across India.

Impact and Threats

Economic Impact: A significant and untaxed drain on the Indian economy, weakening the Rupee and funding a vast criminal underground.

Financial System Integrity: The sheer volume of fraudulent transactions threatens to overwhelm the fraud detection systems of banks and erodes public trust in digital payments.

Social Impact: Indian citizens are victimized twice over—first as targets of the initial scam (gambling, investment fraud) and second as unwitting or coerced money mules who face legal consequences, including frozen accounts and criminal charges.

National Security Threat: This infrastructure can be used to fund activities detrimental to India's national security. The massive data collection by fraudulent apps also represents a significant espionage risk.

Recommendations and Countermeasures

A multi-pronged strategy is essential to dismantle these shadow banking networks.

For Financial Institutions (Banks & Payment Aggregators):

- **AI-Powered Monitoring:** Deploy advanced AI and Machine Learning algorithms to detect patterns indicative of mule account activity (e.g., high velocity of transactions, immediate fund transfers after credit, accounts acting purely as intermediaries).
- **Enhanced KYC/Due Diligence:** Implement stricter video-KYC for corporate accounts and monitor newly opened accounts for suspicious "pass-through" activity in their first 90 days.
- **Information Sharing:** Create a centralized, real-time registry (shared among all banks and law enforcement) of flagged mule accounts and associated individuals/entities to prevent them from operating elsewhere.

For Regulators (RBI, SEBI):

- **Stricter Fintech Regulation:** Impose greater accountability on payment aggregators and fintech platforms to ensure their downstream merchants are not shell companies.
- **Guidelines on Mule Accounts:** Issue clear guidelines defining liability for individuals who "rent" their accounts, while distinguishing between complicit actors and victims.

For Law Enforcement Agencies (LEAs):

- **Capacity Building:** Establish specialized cyber-financial crime units with expertise in blockchain analysis, dark web investigation, and international forensics.
- **International Cooperation:** Actively use diplomatic channels and treaties (like Mutual Legal Assistance Treaties - MLATs) with countries like China, UAE, Cambodia, and Hong Kong to extradite the masterminds.
- **Focus on the Source:** Shift focus from just catching individual mules to dismantling the technical infrastructure and targeting the on-ground agents who recruit them.

For Technology Platforms (Google, Apple):

- **Proactive App Vetting:** Implement a more rigorous and continuous vetting process for apps, especially in the finance, gaming, and "part-time job" categories, before they are listed on app stores.

Public Awareness:

- Nationwide Campaigns: Launch widespread, multi-lingual awareness campaigns educating the public on the dangers of sharing OTPs, banking credentials, or "renting" their accounts. The campaigns must clearly state that being a money mule is a serious criminal offense.

Conclusion

The Chinese-operated illegal payment gateway system is not merely a collection of disparate scams; it is a sophisticated, parallel financial ecosystem that poses a direct challenge to India's regulatory and security framework. Its ability to exploit technology and human vulnerabilities makes it resilient and difficult to eradicate.

Tackling this threat requires moving beyond a reactive stance. A proactive, collaborative, and technology-driven approach is paramount. By strengthening defenses, enhancing investigative capabilities, and fostering international cooperation, India can begin to dismantle this shadow economy and protect its citizens and its financial sovereignty.

Appendix

Detailed breakdown of mule accounts reported

Banks	Mules
India's largest private sector bank by market capitalization	1801
The country's largest public sector lender	9137
A leading public sector bank, recently expanded through a major three-way merger	4631
A major public sector bank, significantly strengthened by a recent three-way amalgamation	2778
The third-largest private sector bank in India	2012
A major Chennai-headquartered public sector bank	1672
A government-owned payments bank operating through the national postal network	1393
A large government-owned bank that recently amalgamated two other public sector banks	1299
A representative group of various smaller private, regional, and cooperative banks operating across the country	21705

Appendix

Non-Exhaustive list of youtube videos endorsing illicit Chinese payment gateways.

S.No.	Title	Channel	Views	Published Date
1	Chinese Payment gateway integration in NODEJS Color prediction website Payin & payout solution	NextTechCraft Solutions	2348	2025-05-22
2	Best Chinese Payment Gateway 2025 Watch Pay Full Integration for Websites [Step-by-Step]	Digital Insaan	819	2025-06-05
3	Chinese payment gateway Chinese payment gateway integration Dragon Pay Chinese getaway	UPI Gateway Coders	123	2025-03-27
4	LG Pay Gateway Setup Full Integration Guide Free Chinese Payment Gateway 2025	Ar It Sulation	635	2025-04-29
5	Chinese Payment Gateway Chinese Payment Gateway Integration Chinese Gateway Payment Gateway	Digital Insaan	5457	2024-12-20
6	Chinese payment gateway Chinese payment gateway integration Dragon Pay Chinese getaway	Neon Tech	558	2025-03-24
7	Free UPI Payment gateway integration in Vuejs Color prediction website Payin & payout solution	NextTechCraft Solutions	2751	2025-05-19
8	Chinese Upi Payment Gateway Fast Upi payment gateway integration UPI payment gateway for website	UPI Gateway Coders	146	2025-03-26

S.No.	Title	Channel	Views	Published Date
9	USDT Payment Gateway with Lowest Fees & Instant Payouts Accept USDT Payments #cryptopayments	Jamsr World	192	2025-05-02
10	Best Payment Gateway for Gambling & Betting Apps Revealed! @PayfromUpiGateway	Pay from Upi Gateway	5476	2024-11-16
11	Exposing the Chinese UPI Gateway Scam Sunpay & Dragonpay Fraud Revealed!	Cxr Smm Enterprises	2673	2025-04-19
12	Color Prediction Website के लिए सबसे भरोसेमंद Chinese Gateway 🔥 (LIVE Proof!)	Cxr Smm Enterprises	5372	2025-05-10
13	How to get chinese payment gateway and aviator game #sunpaygateway #aviatorgame #gatewaysourcecode	Cxr Smm Enterprises	5158	2025-04-06
14	Chinese UPI Gateway Scam Alert SunPay DragonPay Id Fraud Exposed	Zerox Coder	1148	2024-08-28
15	Best Chinese Payment Gateway For Color Prediction Website Payment Gateway For Gaming Website	Techy developer	4363	2025-02-16

Our Capabilities

- **Digital Risk Monitoring:** Real-time visibility and control over your digital assets.
- **External Attack Surface Monitoring:** Detect and mitigate vulnerabilities across 8+ Attack surfaces.
- **Third-party software & Supply Chain Monitoring:** Safeguard vendor ecosystems to prevent Supply chain breaches.
- **Cyber Threat Intelligence:** Proactively identify Indicators of Attack (IOAS) to stop threats in their tracks.
- **Cyber Risk Quantification:** Put a dollar value on potential threats to prioritize mitigation and demonstrate ROI.

95% Faster
Threat Detection

80% Reduced
Response time

Zero
False Positives

200+IAV
Use Cases

Why CloudSEK?

- **Predict Threats Before They Strike:** AI-driven intelligence to identify and mitigate threats at their source-before they become incidents.
- **Comprehensive Coverage:** Monitor 8+ attack surfaces and 200+ Initial Attack Vectors for full-spectrum visibility.
- **Contextual Intelligence:** Unified platform combines Cyber Intelligence, Brand Monitoring, Attack Surface Management, & Supply Chain Risk Analysis for actionable insights.

Trusted by Industry Leaders



& 300+
Organisations



Available in
AWS Marketplace



GDPR
COMPLIANT

