

Notes of Deception: Exposing India's Social Media-Based Counterfeit Currency Network

Category

Adversary Intelligence

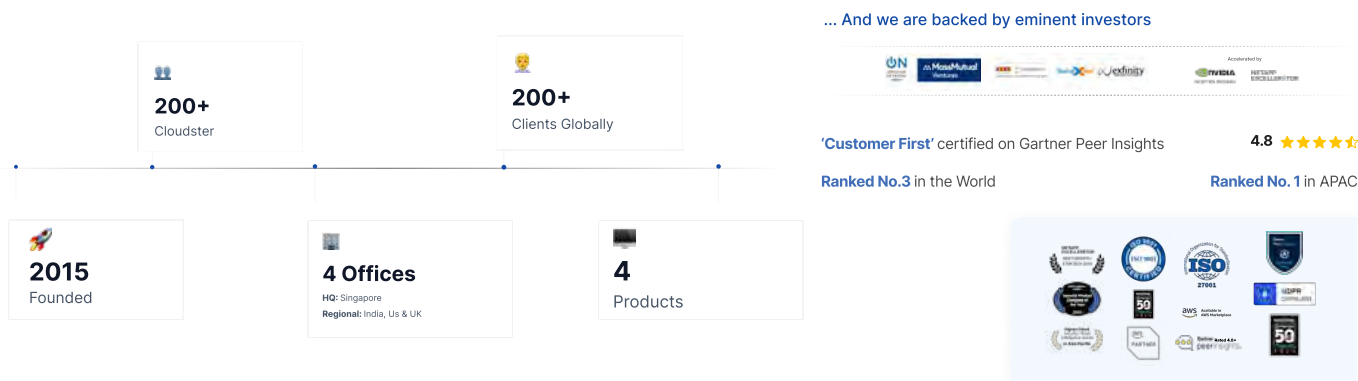
Region

India

Table of Contents	Page No.
1. Executive Summary	03
2. Discovery and Initial Indicators	04-05
3. Analysis Of Facebook Groups	05-07
4. Tactics, Techniques, and Procedures (TTPs)	07-08
5. Potential Fake Currency Production Techniques	08-09
6. Attribution - Facebook Group Administrators	10-13
• First Group	
• Second Group	
7. Attribution - Active Sellers	14-19
• Seller 1	
• Seller 2	
• Seller 3	
• Seller 4	
• Seller 5	
• Seller 6	
8. Correlation Identified	20
9. Estimating The Scale Of Circulation	20
10. Impact of Counterfeit Currency Circulation	20-21
11. Corroborative Evidence from Public Sources	21-22
12. Recommendations - LEAs & Social Media Platforms	22
13. Leveraging CloudSEK Platform - XVigil	23-25
14. Conclusion	25

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.



Executive Summary

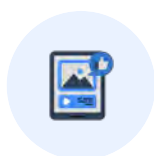
Imagine you're standing at a crowded bank reception, to deposit some leftover cash. Among the notes is a ₹500 bill you received from a local vendor. But this time, the cashier pauses, inspects the note, and informs you that it's counterfeit. You're confused, embarrassed and begin to wonder: Where did this come from? How did it enter everyday circulation? This is not a rare incident anymore. What was once the domain of underground print shops and smuggling networks has now moved online - right into your social media feed.

CloudSEK's STRIKE team has uncovered a widespread campaign where counterfeit Indian currency is being openly marketed and sold across social media platforms. Using OSINT and HUMINT techniques, we attributed and profiled the several sellers, group administrators, revealing their **facial images, exact GPS coordinates, and online identities**.

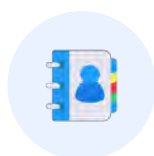
Additionally, data from our XVigil platform uncovered the scale of this illicit ecosystem for the past six months (Dec 26, 2024 – June 26, 2025):

- 4,500+ posts promoting counterfeit currency,
- 750+ accounts/pages facilitating the trade, and
- 410+ unique phone numbers associated with sellers were identified

This whitepaper presents an in-depth analysis of the Tactics, Techniques, and Procedures (TTPs) employed by these actors, along with platform abuse patterns, attribution insights, and the broader implications of digital counterfeit currency networks. It also provides strategic recommendations for law enforcement and digital platforms to counter this emerging threat to India's financial ecosystem.



4500+ posts selling counterfeit currency.



410+ unique phone numbers associated with the sellers.



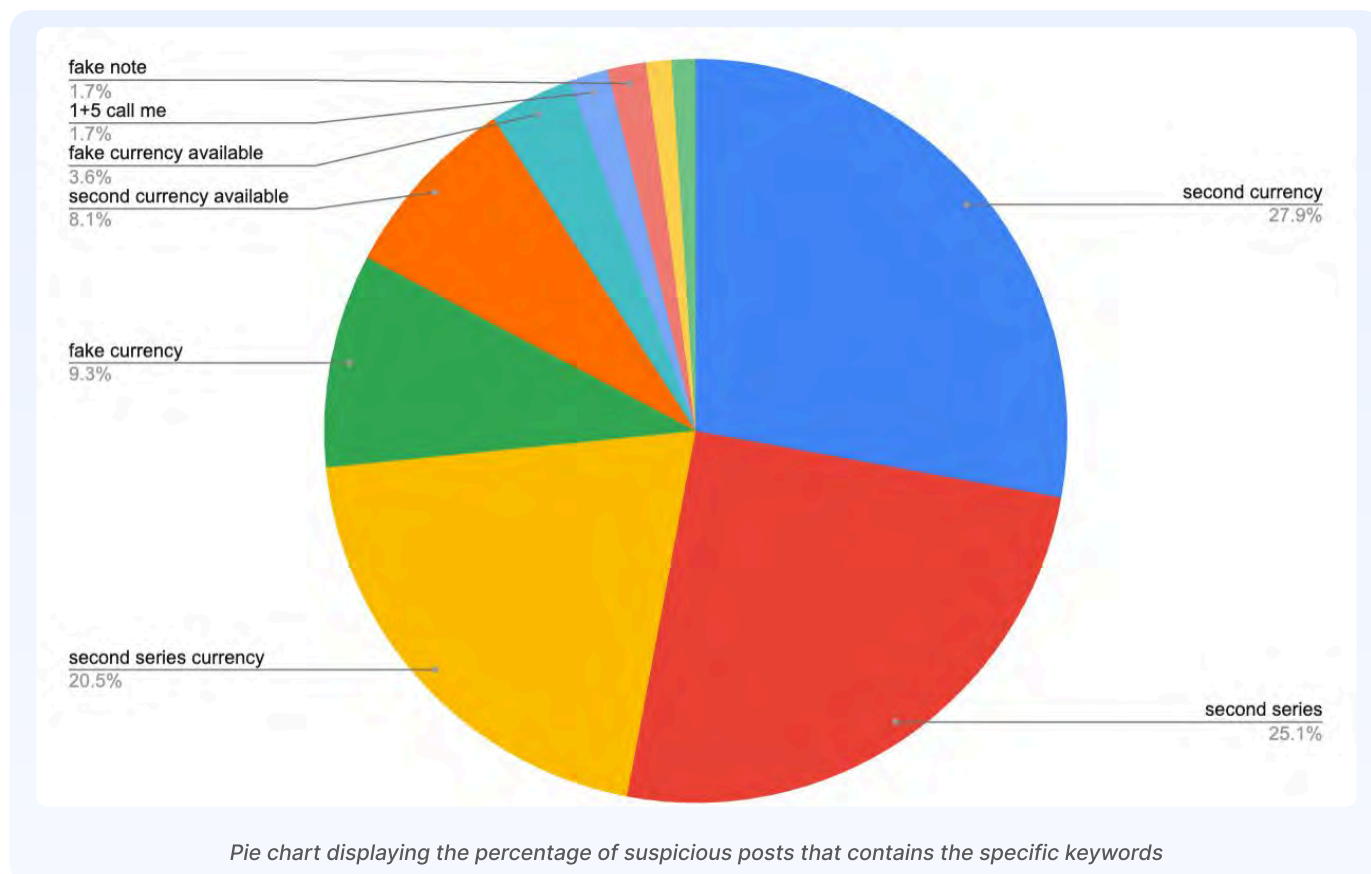
750+ accounts/pages promoting the sale.



Estimated ₹17.5 Crore in Fake Currency Circulated

Discovery and Initial Indicators

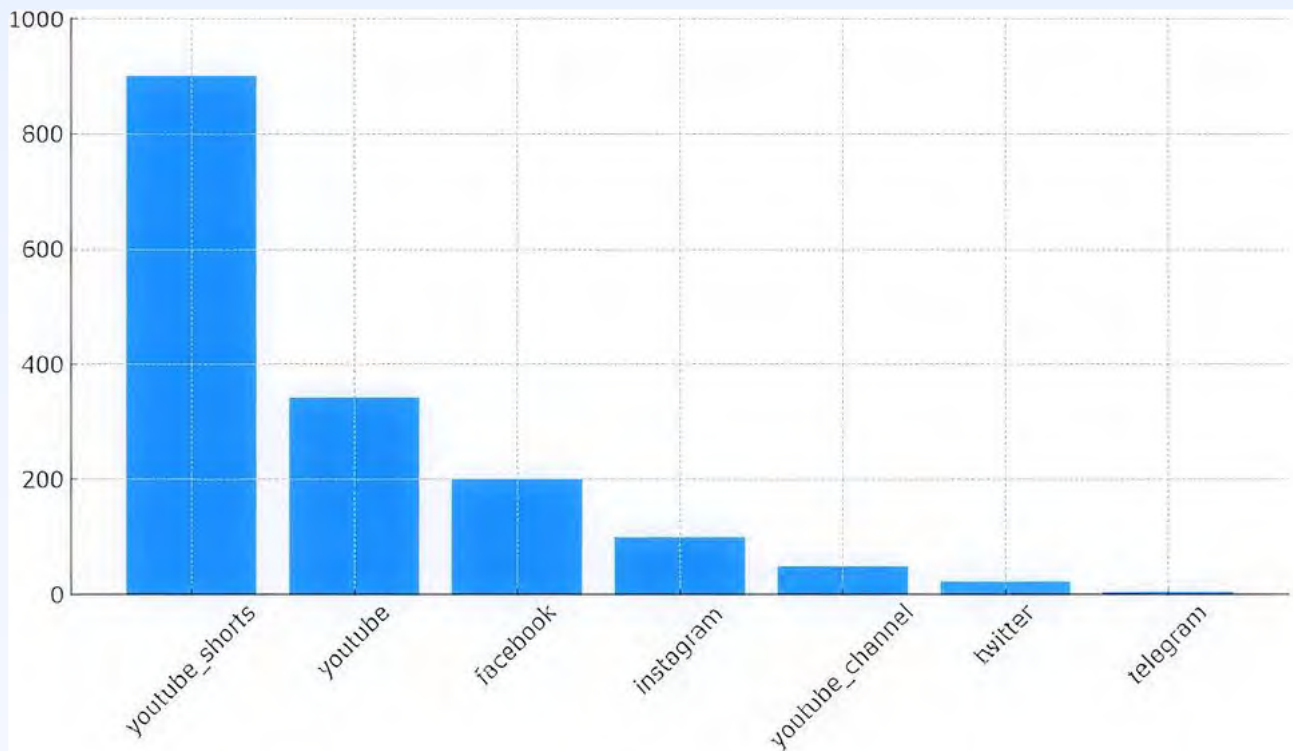
The campaign came to light during CloudSEK's routine monitoring of high-risk keywords and suspicious digital activity. Our digital risk monitoring platform, **XVigil**, had been configured with watchwords such as "second series," "second currency," "fake currency," and other coded terms commonly used as alternatives for counterfeit currency in online spaces.



Once deployed, the platform scanned open-source digital environments for relevant indicators. Over time, it began flagging multiple hits across various social media platforms, pointing towards the presence of suspicious discussions centered around counterfeit currency.

From among the platforms, Facebook stood out because of its diverse ecosystem of pages, personal accounts, and groups, many with thousands of members. Some actors even leveraged Meta Ads to promote their offerings, highlighting the platform as a major hub for such illicit activity.

This volume of publicly available data provided a rich landscape for deeper analysis, prompting us to prioritize Facebook for extended monitoring and profiling, which ultimately led to the uncovering of the broader counterfeit currency network detailed in this report.

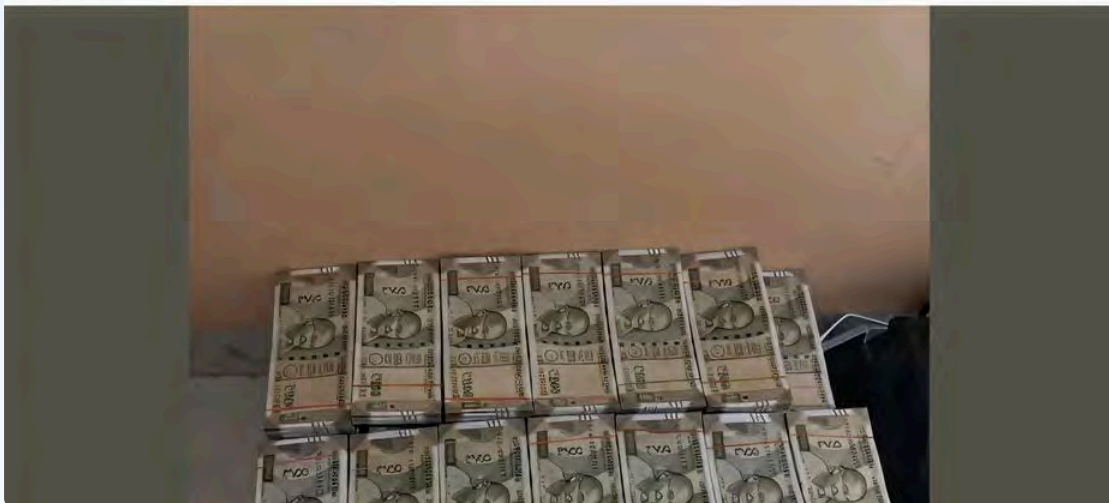


Bar chart displaying the number of posts under different social media platforms containing phone numbers to contact the seller

Analysis Of Facebook Groups

Upon deeper analysis, these groups displayed clear indicators of criminal intent, with **members openly advertising fake Indian currency**, price ranges, delivery options, and contact numbers. Unlike dark web marketplaces, this activity was not hidden behind anonymized networks - it was occurring in plain sight, on public platforms.

1+4 . Mumbai.. Delhi... Lucknow... Rajasthan..up.. Hyderabad... Bihar..8828513767 WhatsApp call me



Snapshot of a post claiming the availability of counterfeit currency in multiple different states/cities

Analysis of multiple posts revealed a recurring pattern in pricing: for **every ₹1,00,000 paid in genuine currency**, buyers were promised **₹5–8 lakhs in counterfeit notes**. Several posts boldly claimed that the counterfeit currency was “A1 quality,” capable of bypassing Cash Deposit Machines (CDMs), ATMs, and standard counterfeit detection mechanisms asserting that all security features such as watermarks, color-shifting ink, and security threads were accurately replicated.

1+8 second currency notes available CDM PASS market pass A1 quality face to face 🔄 hand to hand 🔄 deal 🔄 check karke milega function to function real note interested person contact me 1 lakh ka 8 lakh milega March offer offer offer offer offer offer offer offer offer offer offer offer offer offer offer 🔄 🔄 🔄 8999749613

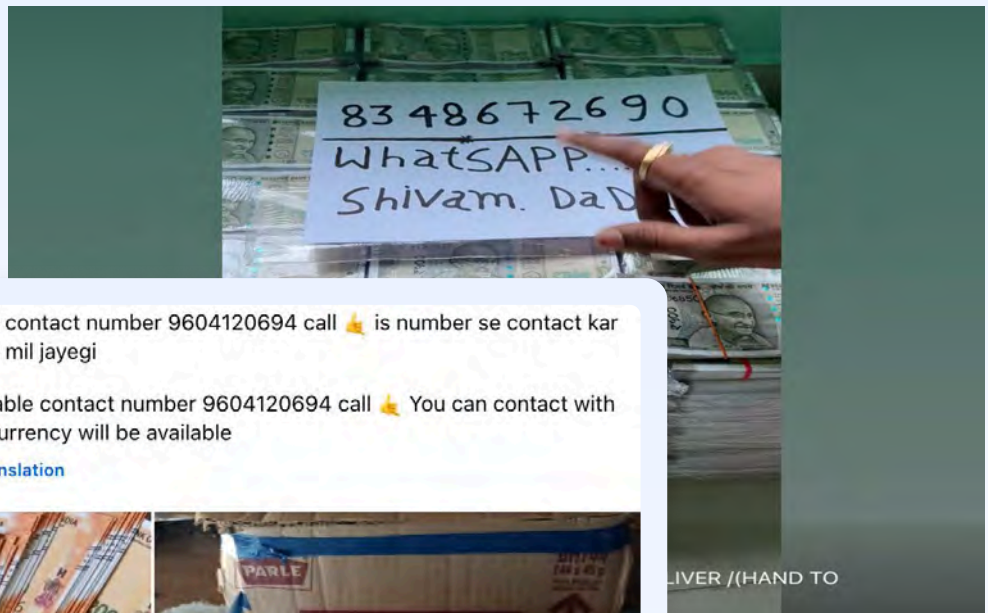


Snapshot displaying a post claiming that the counterfeit currency can bypass CDM checks and the seller is ready for a hand to hand deal

Note : A1 quality counterfeit currency refers to fake money produced with exceptional precision to closely mimic genuine banknotes. It features high-resolution printing, authentic-feeling paper, accurate colors and layouts, clean-cut edges, and convincingly replicated security elements like watermarks, holograms, and microprinting making it difficult to detect by sight, touch, or basic machines.

Moreover, several individuals have also shared images displaying stacks of counterfeit currency alongside a handwritten note or a phone screen showing their personal contact number. This tactic is commonly used to build trust with potential buyers, serving as supposed “**proof of legitimacy**” to assure them that the seller actually possesses the fake currency and is not attempting to scam them.

Snapshot of a Facebook video displaying the seller's number placed on the counterfeit currency as a proof of legitimacy



1+10+chicken currency available contact number 9604120694 call 📞 is number se contact kar sakte ho second series currency mil jayegi

1+10+chicken currency available contact number 9604120694 call 📞 You can contact with this number, second series currency will be available

⚙️ Hide Translation · Rate this translation



Snapshot of a Facebook post displaying the seller's number placed on the counterfeit currency as a proof of legitimacy

Tactics, Techniques, and Procedures (TTPs)

Based on detailed analysis and direct engagement with the threat actors, the following Tactics, Techniques, and Procedures (TTPs) were identified as part of their ongoing counterfeit currency distribution operations:

- **Promotion:** Threat actors promote counterfeit currency using Youtube, Facebook groups, personal Facebook accounts, Instagram profiles and also run Meta Ads. They frequently utilize Instagram Reels, Facebook and Youtube Shorts, embedding trending hashtags such as #currency, #counterfeit, #fakecurrency, and #fakecurrencynotes to increase visibility and reach a broader audience.
- **Engagement:** Initial engagement typically occurs over WhatsApp or direct phone calls. To build trust, the sellers often share images of the counterfeit notes featuring handwritten notes with their phone number, and may even offer video calls to show the cash live - serving as a tactic to appear credible.

- **Payment:** Transactions are usually negotiated to occur in person, where buyers are encouraged to first inspect the counterfeit currency before making the payment. While some actors offer Cash on Delivery (COD), others demand a pre-booking amount in advance (a method frequently associated with scams and frauds).
- **Delivery:** Delivery methods vary and include dead drops, face-to-face handovers at pre-decided locations, and, in some cases, the use of courier services for discreet delivery.
- **Operational Security Measures:** Actors behind these campaigns often maintain multiple fake social media profiles, use pseudonyms, fraudulent identity cards, and burner phone numbers to conceal their true identities and avoid detection.
- **Risks and Threat Actor Behavior:** Some cases have escalated into robberies or physical threats during in-person meetings. Several sellers exhibit intimidating behavior and claim to have local connections or criminal affiliations, which they use to pressure or manipulate buyers. This highlights an additional layer of risk associated with offline interactions in such campaigns.

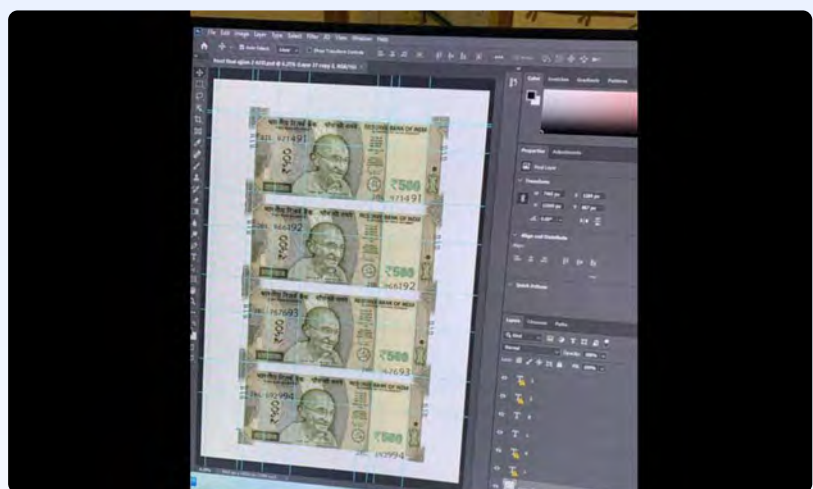
Potential Fake Currency Production Techniques

Based on open-source observations, it was found that several sellers involved in this underground network have also showcased the materials and methods used to manufacture counterfeit Indian currency.

Some sellers posted images of the specialized paper used for printing fake notes. Alarming, this paper appears to come pre-fabricated with security features such as the **Mahatma Gandhi watermark** and the **green security thread**, closely mimicking legitimate Indian currency paper.



Snapshot of the paper containing watermark and security thread



Snapshot displaying the usage of Adobe photoshop to design the counterfeit currency

Further investigation revealed that design software like **Adobe Photoshop** is widely used to recreate or manipulate note designs. In certain cases, sellers were even seen advertising and selling **PSD (Photoshop Document) files**, which can be directly edited to produce high-quality replicas of various denominations.

Once the design is finalized, **it is printed using large-format, high-resolution printers** capable of producing bulk quantities of counterfeit notes. These printers, typically used for commercial printing jobs, allow for the mass replication of currency with deceptive visual accuracy.



Snapshot from a video displaying the printing of the currency

This combination of access to authentic-looking materials, digital design tools, and industrial-grade printers poses a serious threat, as it enables individuals or groups to scale their operations while maintaining a level of sophistication that can evade basic detection.

Attribution - Facebook Group Administrators

CloudSEK's researchers identified a large number of Facebook groups actively engaged in promoting and selling fake Indian currency. From this pool, two groups were shortlisted for deeper investigation: **"Fake India Second Hand Currency Available WhatsApp Number Call 7559336902"** and **"Fake Indian Currency Contact Mobile Number 8265032575."** These groups were chosen based on several key indicators - the high number of members, consistent posting frequency, and the visible activeness of group administrators in engaging with potential buyers.

First Group

Group's Name	fake Indian currency contact mobile number 8265032575
Date Created	13 Aug 2024
Number Of Members	1100+
Admin Alias	Vivek Kumar
Frequency Of Posts	Medium
Activeness Of Group Admin	High

Further investigation into the Facebook profile of the group administrator, identified as **Vivek Kumar**, revealed numerous posts openly promoting the sale of counterfeit currency. These posts included detailed descriptions and a consistent phone number for contact. Leveraging a combination of HUMINT and OSINT techniques, CloudSEK's analysts were able to uncover Vivek Kumar's extended social media footprint, obtain his facial photograph, and pinpoint his exact GPS coordinates, leading to a high-confidence attribution.

Alias	Vivek Kumar, Anand Kedia, Songadh Vyara
Contact Number	+917822978380, +918265032575
Facebook Account	https://www.facebook.com/vivek.kumar.283420+
Instagram Account	https://www.instagram.com/iamvivekkumar7/
Latitude	21.2146251
Longitude	74.3404639
Google Maps	https://www.google.com/maps/place/21.2146251,74.3404639



fake Indian currency contact mobile number 8265032575

Public group · 1.1K members

Join Group

Share



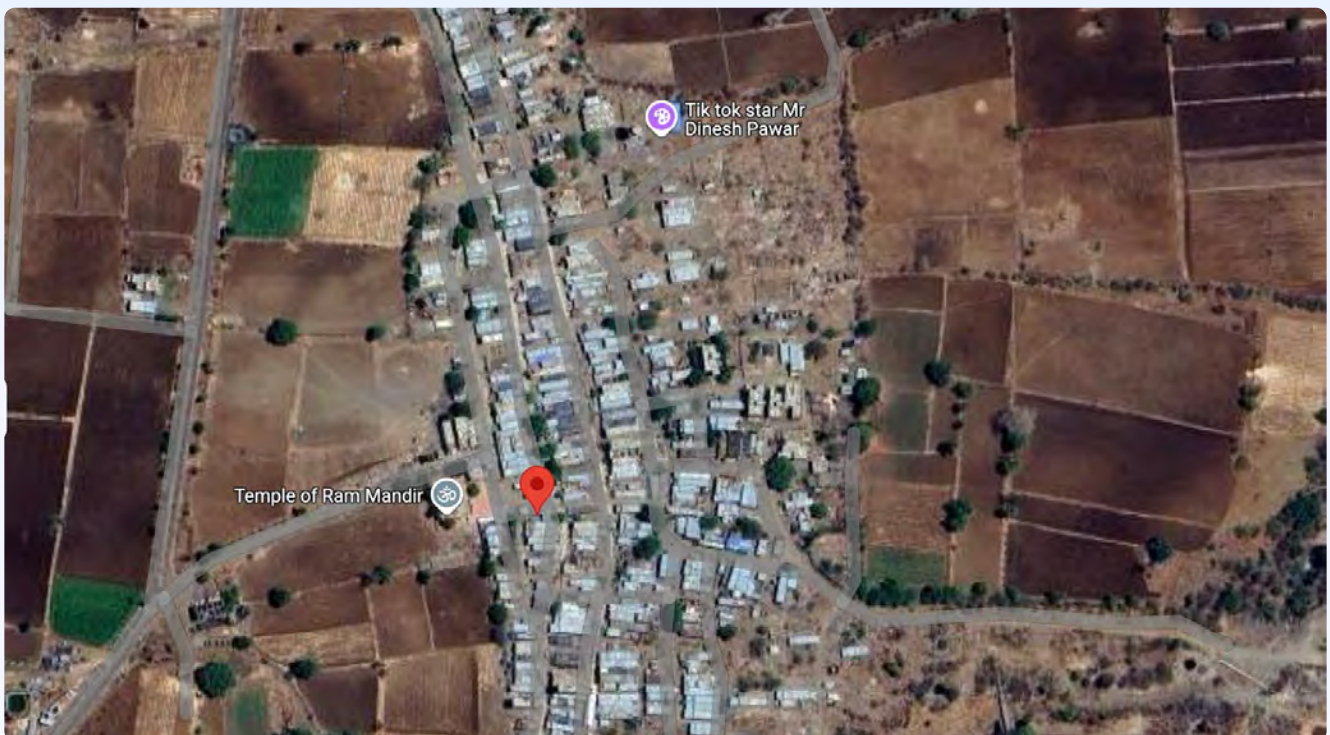
Snapshot of the Facebook group



Snapshot of Vivek Kumar's Facebook post



Front camera picture of Vivek Kumar




Exact GPS location of Vivek Kumar

Second Group

Group's Name	Fake India Second Hand Currency Available WhatsApp Number Call 7559336902
Date Created	2 Aug 2024
Number Of Members	751+
Admin Alias	Karan Pawar
Frequency Of Posts	High
Activeness Of Group Admin	High

Using the same OSINT and HUMINT methodologies, another admin with the alias **Karan Pawar** was identified and attributed. His profile exhibited similar patterns - multiple posts promoting counterfeit currency.

Alias	Karan Pawar, Surya Pawar, Robin Pawar
Contact Number	+917559336902
Facebook Account	https://www.facebook.com/profile.php?id=100091250097454
Instagram Account	https://www.instagram.com/suryapawar811/
Telegram Handle	@Robinpawar07
Instagram Threads Account	https://www.threads.com/@suryapawar811
Latitude	21.21437
Longitude	74.34102
Google Maps	https://www.google.com/maps/place/21.21437,74.34102



Group by Karan Pawar

fake India second hand currency available WhatsApp number call 7559336902

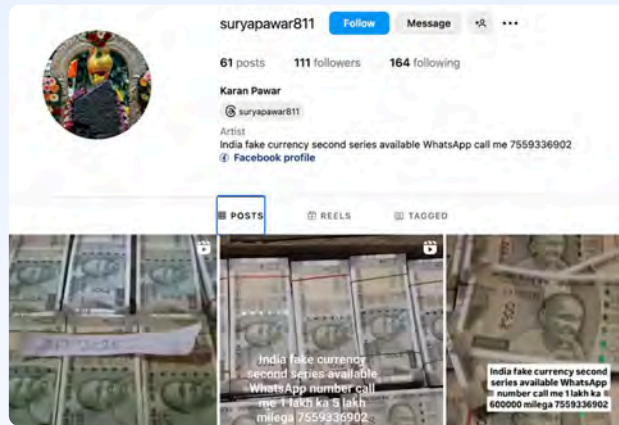
Public group · 751 members

Join Group Share

Snapshot of the Facebook group



Snapshot of Karan Pawar's Facebook post



Snapshot of Karan Pawar's Instagram post



Front camera picture of Karan Pawar



Karan Pawar's picture extracted from Facebook



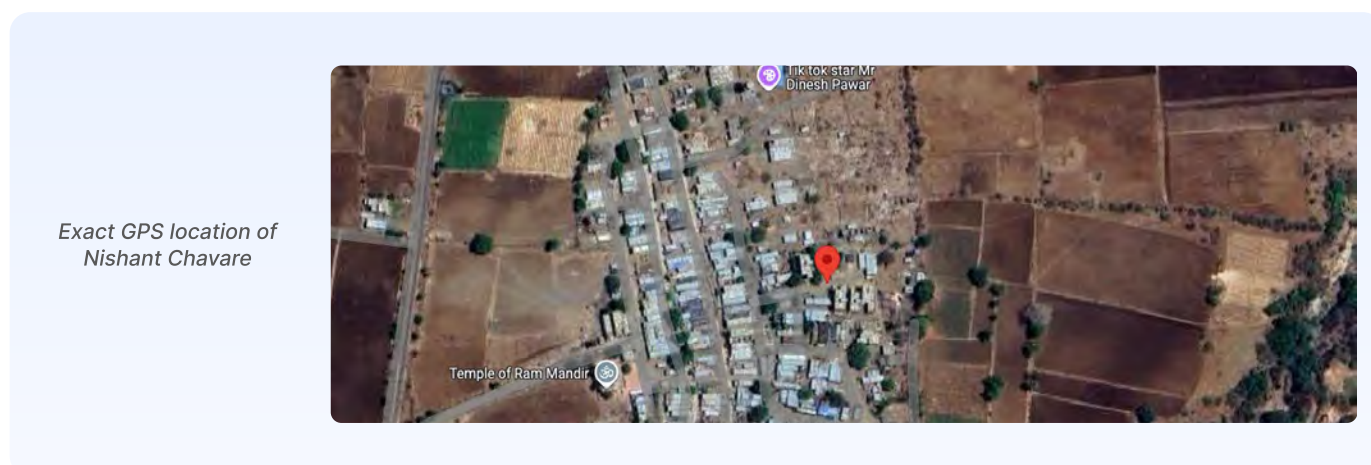
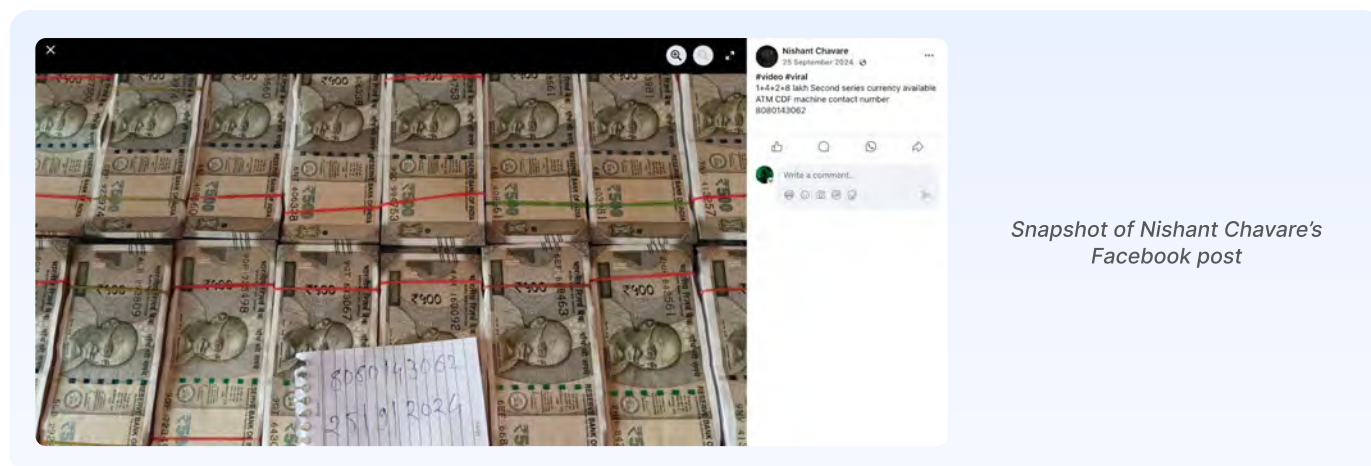
Exact GPS location of Karan Pawar

Attribution - Active Sellers

In addition to the primary administrators, we also decided to attribute a few other active sellers involved in the counterfeit currency network. However, the degree of attribution varied across individuals. In some cases, we were able to identify their location but not their facial identity, while in others, we managed to obtain a clear image but couldn't confirm their exact whereabouts. Despite these limitations, their repeated activity, consistent communication patterns, and engagement across multiple groups firmly establish their role in the broader campaign.

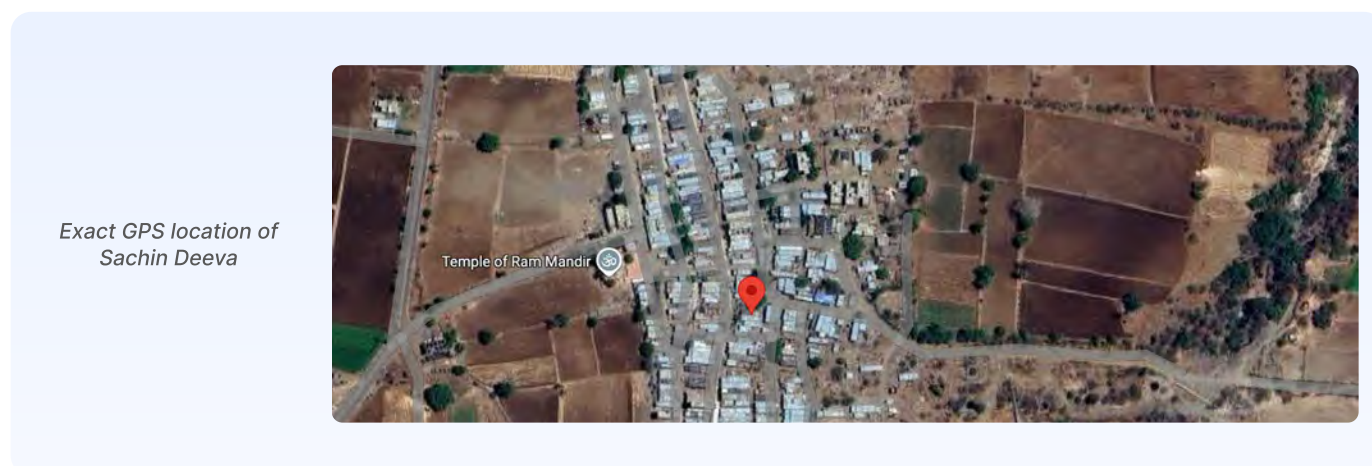
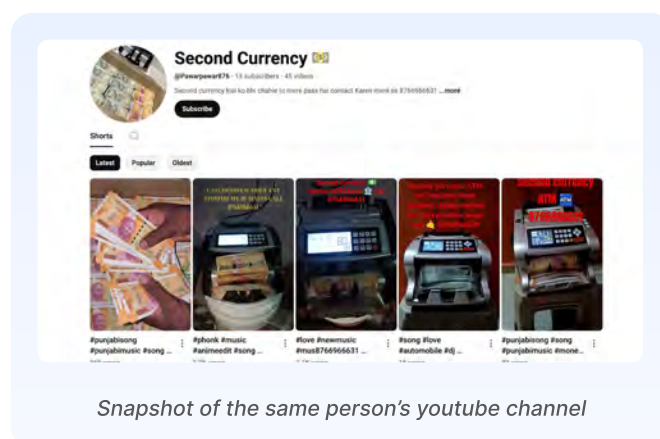
Seller 1

Alias	Nishant Chavare
Contact Number	+918080143062
Facebook Account	https://www.facebook.com/profile.php?id=100027398435224
Instagram Account	https://www.instagram.com/nishantchaure8080
Latitude	21.215292821515593
Longitude	74.34154480906278
Google Maps	https://www.google.com/maps/place/21.215292821515593,74.34154480906278



Seller 2

Alias	Pawar Pawar, Dinshkumar Saroj, Sachin Deeva
Contact Number	+918766966631
Facebook Account	https://www.facebook.com/sachin.deeva.750
Youtube Channel	https://www.youtube.com/@Pawarpawar876
Latitude	21.21470474384334
Longitude	74.34087087150408
Google Maps	https://www.google.com/maps/place/21.21470474384334,74.34087087150408



Seller 3

Alias	Gotam Pawar, Rakesh Pawar
Contact Number	+917498258431
Facebook Account	https://www.facebook.com/dipupawsr1212
Instagram Account	https://www.instagram.com/nishantchaure8080
Latitude	20.80663
Longitude	74.63422
Google Maps	https://www.google.com/maps/place/20.80663,74.63422



Snapshot of Gotam Pawar's Facebook post



Front camera picture of Gotam Pawar



Gotam Pawar's picture from Truecaller




Exact GPS location of Gotam Pawar

Seller 4

Alias	Tukaram Rm, Gopal Kumar, Aashiq Laila
Contact Number	+919604120694
Facebook Account 1	https://www.facebook.com/profile.php?id=61559372313080
Facebook Account 2	https://www.facebook.com/profile.php?id=61574189369929
Instagram Account	https://www.instagram.com/si.taram3321/
Latitude	21.0308683
Longitude	76.35246
Google Maps	https://www.google.com/maps/place/21.0308683,76.35246

1+10+5+50 second currency mil jayegi contact number 9604120694 diye hue number per contact kar sakte ho

See translation

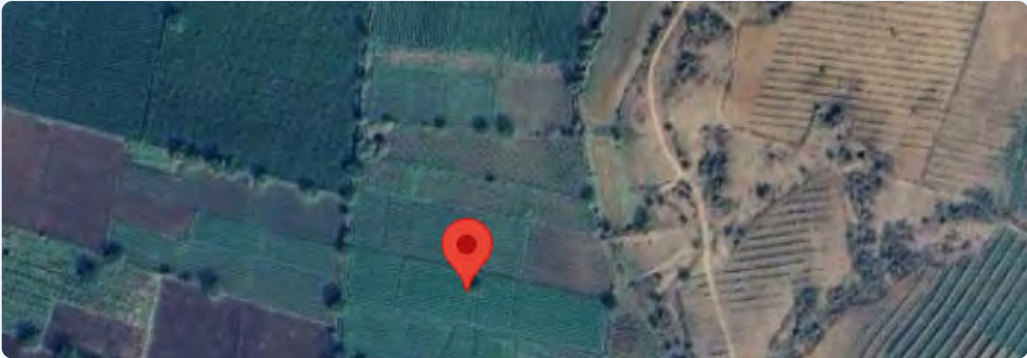


Snapshot of Tuka Rm's Facebook post



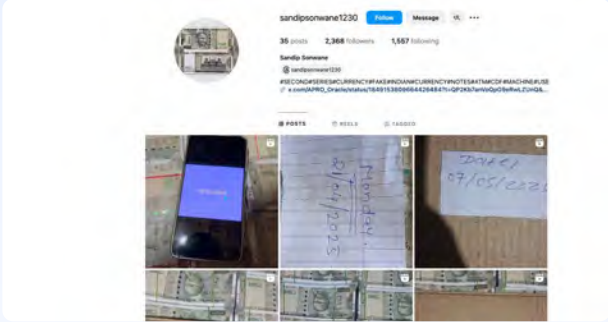
Front camera picture of Tuka Ram

Exact GPS location of Tuka Ram



Seller 5

Alias	Sandip Sonawane
Contact Number	+918208318742
Instagram Account 1	https://www.instagram.com/sandipsonwane1230/
Latitude	18.4326404
Longitude	73.8599666
Google Maps	https://www.google.com/maps/place/18.4326404,73.8599666



Snapshot of Sandip Sonawane's Instagram profile



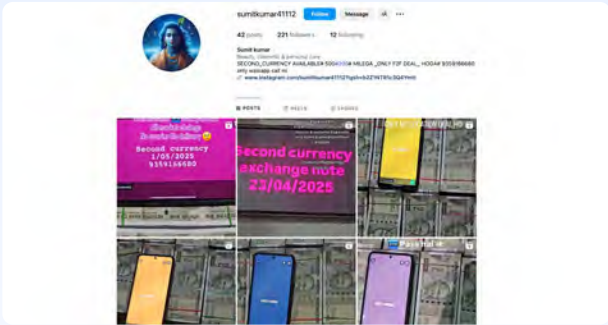
Front camera picture of Sandip Sonawane

Exact GPS location of Sandip Sonawane

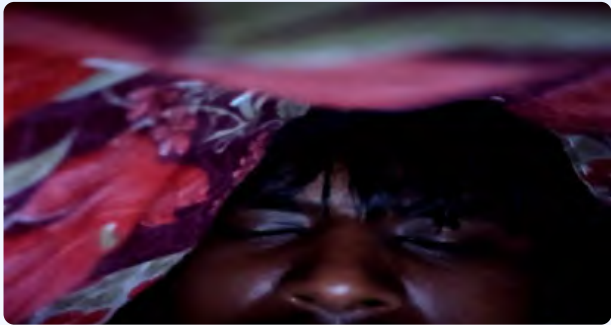


Seller 6

Alias	Madhav Gaikwad, Sumit Kumar
Contact Number	+919359166680
Instagram Account 1	https://www.instagram.com/madhavgaikwad485
Instagram Account 1	https://www.instagram.com/sumitkumar41112/
Email	saileshkumar58778@gmail.com



Snapshot of Sumit Kumar's Instagram profile



Front camera picture of Sumit Kumar

Correlation Identified

Based on the detailed attributions conducted during this investigation, a significant geographic clustering was observed. Two group administrators, two confirmed sellers, were all found to be located in or around **Jamade Village, in Dhule district, Maharashtra**. Additionally, one individual was traced to **Pune**, while two others could potentially be operating from areas in close proximity to **Dhule**.

This geographic overlap strongly suggests the presence of a coordinated counterfeit currency syndicate operating primarily out of **Maharashtra**, with **Dhule** emerging as a potential hotspot for such activities.

Estimating The Scale Of Circulation

Our analysis reveals **over 410 unique phone numbers** in the last 6 months associated with individuals selling counterfeit currency. Assuming some individuals operate multiple contact points, we conservatively estimate this network comprises around **350 distinct sellers**.

These sellers typically offer counterfeit currency at a conversion rate - for every ₹1 lakh in genuine money, buyers may receive between ₹5 to ₹8 lakh in fake notes. Even using the lower bound of ₹5 lakh per transaction, this implies that each seller could be responsible for **circulating at least ₹5 lakh** in counterfeit currency.

By extrapolating this figure across 350 individuals, we arrive at a minimum estimated circulation of **₹17.5 crores in counterfeit currency** over a six-month period.

It is important to note that this is a conservative estimate. The true volume may be significantly higher or lower, influenced by factors such as transaction frequency, buyer demand, and varying exchange rates in these illicit transactions. While speculative, this extrapolation illustrates the potentially vast financial impact and serious societal risk posed by such operations.

Impact of Counterfeit Currency Circulation

- **Economic Destabilization** : The unchecked spread of counterfeit currency inflates the money supply without corresponding value, which can lead to inflationary pressures. This erodes public trust in the monetary system and undermines the credibility of the national currency.
- **Financial Loss to Individuals and Businesses** : Unsuspecting individuals and small businesses often suffer direct financial losses when they unknowingly accept fake notes, which are later rejected by banks or authorities. For low-income earners, even one counterfeit note can cause significant hardship.

- **National Security Threat** : The circulation of counterfeit currency can be tied to organized criminal networks or foreign hostile entities aiming to destabilize the economy. It may also be used to fund illegal activities, such as terrorism, narcotics, or arms trade, posing a serious threat to national security.
- **Burden on Law Enforcement and Financial Institutions** : Tackling the spread of counterfeit money consumes considerable resources from law enforcement agencies, intelligence bodies, and central banks. It necessitates increased surveillance, forensic efforts, and policy interventions, diverting attention from other critical security needs.
- **Erosion of Public Confidence** : As fake notes enter common circulation, people become increasingly suspicious of cash transactions, especially with high-denomination notes. This not only affects day-to-day commerce but can also weaken the cash-based segments of the economy, particularly in rural or underbanked areas.

Corroborative Evidence from Public Sources

The findings of this investigation are further substantiated by multiple local news reports that highlight past incidents involving counterfeit currency in and around the Dhule district of Maharashtra. These reports indicate that the region has, over time, witnessed a recurring pattern of counterfeit currency circulation and law enforcement crackdowns on organized counterfeiting operations.



Pudhari News

<https://pudhari.news> > ... > धुळे · [Translate this page](#) ⋮

Dhule Crime | Fake money worth Rs 25 thousand seized from youth in Dhule

16 Mar 2025 — Dhule: Fake currency notes worth around Rs 25,000 have been seized from a youth near a hotel on the Nagpur-Surat highway in Dhule . A case has been registered against the youth and...

[Source](#) ↗



Pudhari News

<https://pudhari.news> > crimediciary · [Translate this page](#) ⋮

Dhule Crime | 24 people arrested in fake currency case in Dhule district

7 May 2025 — Dhule Crime | 24 people booked in fake currency case in Dhule district ... Dhule: Fraudsters have been arrested on social media for allegedly offering fake currency, gold, copper wire a...

[Source](#) ↗



Pudhari News

<https://pudhari.news> › crimediary · [Translate this page](#) ⋮

Dhule Crime News | Fake notes of five lakhs seized in Shirpur

4 Feb 2025 — Fake notes worth around Rs 4,11,500 were found in Shirpur city. It has been fo the fake note racket came from Gujarat state to Nashik district and from there to Shirpur in Dh

[Source](#) ↗



TV9 Marathi

<https://www.tv9marathi.com> › dhul... · [Translate this page](#) ⋮

Dhule police take major action, bust a gang manufacturing fake currency notes

28 Oct 2020 — (**Dhule** police take a Action against four Accused in **fake Currency** racket). Related News. Pune Crime | Pune Fake Currency ...

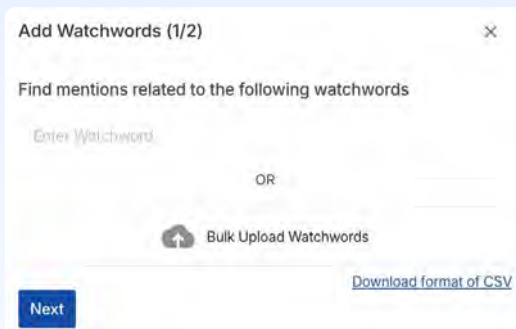
[Source](#) ↗

Recommendations - LEAs & Social Media Platforms

- **Proactive Monitoring** : Law enforcement agencies should actively monitor social media platforms, underground marketplaces for such campaigns using advanced threat intelligence platforms like CloudSEK XVigil, which can detect malicious content, fake profiles, and coordinated campaigns in real time, enabling quicker identification and takedown of illicit activities.
- **Launch Targeted Investigations** : Based on attribution data, initiate on-ground operations in Dhule district, Jamade Village and nearby areas in Maharashtra, which appear to be a hotspot for this counterfeit currency syndicate.
- **Monitor Identified Individuals and Numbers** : Use the gathered phone numbers, profile details, and facial images to place suspects under surveillance and investigate their broader criminal networks and financial flows.
- **Immediate Takedown of Identified Groups and Accounts** : Meta, Google and other Social Media platforms should be alerted to remove the different Facebook groups/posts, Shorts and related Instagram accounts promoting counterfeit currency, based on evidence from this investigation.
- **Strengthen Monitoring of Hashtag-Based Promotions** : Social Media platforms must use pattern detection and image/video analysis to identify and block reels, shorts, and posts using hashtags like #fakecurrency, #a1note, #counterfeitindia.
- **Monitor Meta Ad Library for Illegal Campaigns** : Ads promoting counterfeit currency were discovered - platforms must monitor the approved advertisements more strictly, especially when finance-related content is advertised.

Leveraging CloudSEK Platform - XVigil

This investigation into counterfeit currency distribution operations was significantly aided by the **CloudSEK XVigil** platform, which provided end-to-end visibility across a wide range of digital sources. By configuring a targeted set of watchwords, XVigil enabled continuous monitoring across social media and messaging platforms, dark web, paste sites, and other online forums.

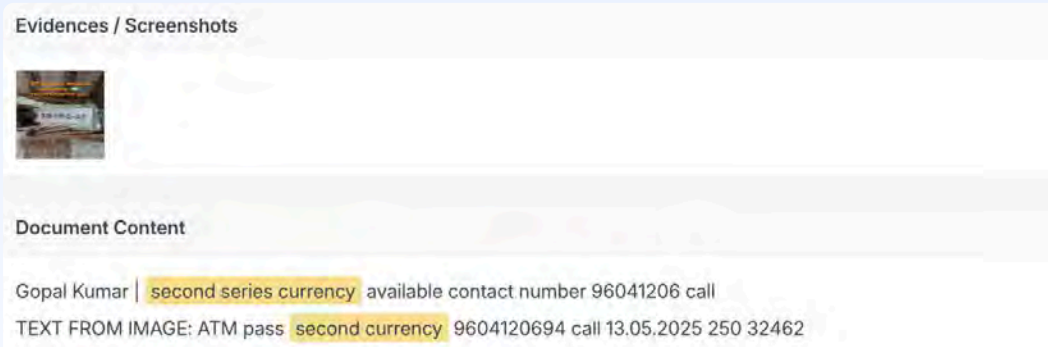


Snapshot displaying the “Add Watchwords” feature

Using XVigil’s **Fake Call Center module**, it was possible to identify posts on platforms like Youtube, Facebook, Telegram, Instagram etc that contain phone numbers associated with counterfeit currency sellers. These phone numbers, once detected, could be further added as new watchwords, expanding the scope of monitoring and allowing for the development of detailed threat actor profiles.



Snapshot displaying an event under Fake Call Centres module of XVigil



Snapshot displaying the evidence and document content of the event

The platform's **Fake Pages & Channels** module was also used to identify accounts and pages with names that matched the watchwords.

Event Details	
Module	Scan Date & Time
Fake Pages and Channels	28 May, 2025 05:25:01 AM
Source Name	
facebook	
Source URL	
https://www.facebook.com/people/fake-currency-इंडिया/61576368973990	
Matched Assets	
fake currency	

Snapshot displaying an event under Fake Pages and Channels module

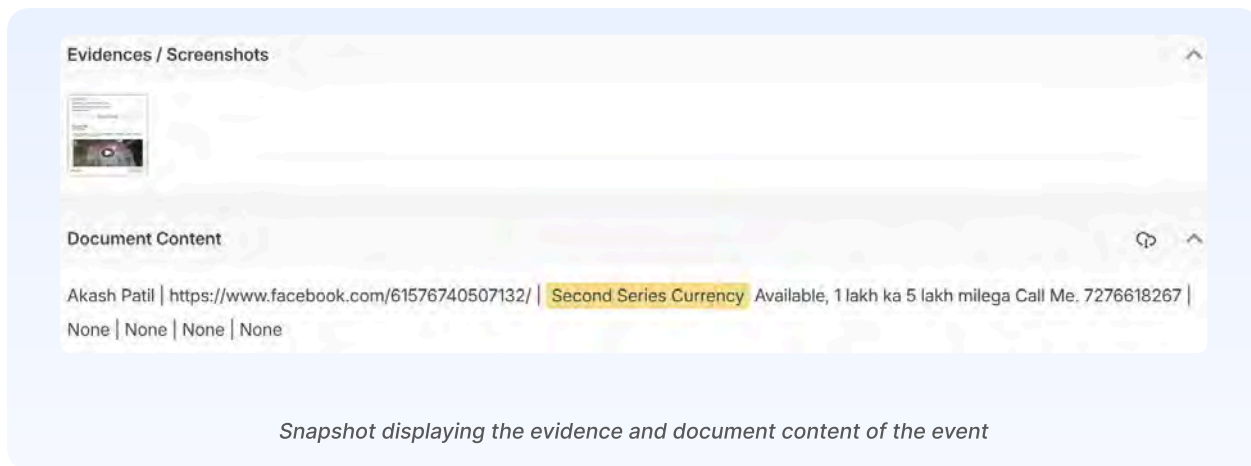
Document Content	
https://www.facebook.com/people/fake-currency-इंडिया/61576368973990	fake currency इंडिया None None None
fake currency इंडिया	
Internet marketing service	
1 लाख का 4 लाख fake currency	हैंड टू हैंड डील #वायरल #post #पब्लिक

Snapshot displaying the document content of the event

Furthermore, XVigil also uncovered several **Meta Ads** promoting counterfeit currency, providing insight into how paid advertising was used to reach a broader audience.

Event Details	
Module	Scan Date & Time
Fake Pages and Channels	25 May, 2025 06:03:56 AM
Source Name	
facebook	
Source URL	
https://www.facebook.com/ads/library/?id=2750606458465258	
Matched Assets	
second series second series currency	

Snapshot displaying an event under Fake Pages and Channels module



Snapshot displaying the evidence and document content of the event

This multi-layered approach, combining keyword-based detection along with HUMINT and OSINT enabled comprehensive mapping and profiling of the threat landscape. This intelligence was crucial in understanding the tactics, reach, and operational structure of the actors behind the counterfeit currency campaign.

Conclusion

This report is an effort to shed light on how crimes with the potential to severely impact national security are unfolding in plain sight - on public social media platforms, without restraint. The cases detailed here represent only a fraction of a much larger ecosystem. Dozens of other groups, sellers, and accounts continue to operate daily, fueling a black market that threatens economic integrity and public safety. Addressing this growing threat requires more than reactive takedowns. Only through continuous monitoring by law enforcement, coordinated cross-agency efforts and stronger case based content moderation by platforms can such networks be disrupted before they expand beyond control.

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

nasscom

NIC National Informatics Centre

EMAAR

NetApp

MetLife

& 300+ Organisations



#1 Threat Intelligence Vendor in APAC | Rated 4.5+
Gartner
Peer Insights



Available in
AWS Marketplace

