OSINT Casefile: indiangigoloclub.com
Fraud Intelligence Portfolio
Author: Rohin Vachani
Date: 6-12-2025

Analyst Preface

This casefile is part of my threat and fraud intelligence portfolio. It demonstrates how I approach real-world investigations using only passive OSINT, limited public data, and first-principles reasoning. The objective is not to uncover every hidden detail but to show how I extract patterns, reconstruct workflows, and model the structure of an operation when the available information is incomplete.

This report stands on its own and contains all methodology, findings, analysis, and conclusions required to understand the operation behind the domain.

Executive Summary

This casefile presents a passive, open-source investigation into indiangigoloclub.com, a domain with a high concentration of fraud complaints on consumercomplaints.in. All visible signals point to a two-layer structure: a central lure (the website) that attracts victims at scale, and a distributed network of independent scammers who conduct the actual financial extraction using temporary UPI mules and throwaway phone numbers.

The complaints follow the same procedure but differ sharply in execution—different document styles, different payment patterns, different pressures, and different story variations—which strongly suggests multiple operators using the same basic outline rather than one coordinated team. The website remains stable and unchanged over time, while the scammers behind it vary from case to case.

Because this investigation was intentionally limited to passive OSINT and a single complaint source, deeper attribution or cross-platform mapping is not possible here. Within those limits, the evidence supports one conclusion: the domain exists to generate leads, and the fraud is carried out by multiple operators who use it as a starting point.

Why This Domain Was Selected

The domain had an unusually high number of complaints, many describing similar patterns of financial loss. These complaints included screenshots, IDs, WhatsApp chats, and UPI trails, making it a suitable choice for extracting operational behaviour using only passive OSINT.

Source of Complaint Data

All complaint data comes specifically from consumercomplaints.in.
No other platforms, forums, or datasets were used.
This was intentional to show how much intelligence can be extracted from a single, consistent source.

Methodology

This casefile was developed entirely through passive OSINT. The investigation relied on:

- WHOIS, DNS, MX, and hosting lookups
- Complaints and screenshots shared on consumercomplaints.in

The approach involved:

1. Observing raw signals
2. Identifying repeating behavioural shapes
3. Filtering irrelevant or inconsistent details
4. Reconstructing the workflow seen across complaints
5. Modelling the likely structure based on the available patterns

The investigation remained intentionally narrow to emphasise reasoning instead of volume.

Infrastructure Analysis

Tools Used

- dig
- viewdns
- Standard WHOIS lookups

Domain Characteristics

- Created in 2015
- Active and maintained

- WHOIS privacy enabled through Domains By Proxy

The long lifespan suggests the domain is intended to remain online as a stable lure rather than as a disposable scam domain.

Hosting and DNS

- Hosting: Hostinger (AS47583)
- IP geolocation: Mumbai
- Nameservers: default Hostinger/parking
- Mail: default Hostinger MX
- Subdomains: autoconfig, autodiscover, mail (auto-generated)

The configuration is simple and low-cost. There is no CDN, reverse proxying, or other signs of technical sophistication. The hosting IP is part of a shared hosting range.

Content Observations

The website claims presence across many Indian cities. The content is broad, repetitive, and designed to attract a large volume of inquiries.
The **contact button** is likely the main pivot that transfers the victim from the website to WhatsApp, where the scam begins.

Interpretation

The infrastructure supports the idea of a long-running lure designed to generate steady victim traffic. The technical setup does not indicate a large or sophisticated operation but instead a simple entry point that feeds downstream scammers.

Complaint Analysis

Complaints originate from multiple regions across India, consistent with the website's claimed coverage.

Evidence Shared by Victims

Victims provided:

- WhatsApp conversations
- UPI payment confirmations
- Edited certificates and membership documents
- Edited ID cards for “agents” and “clients”
- Fabricated hotel confirmations
- Tiered membership structures

The formats and styles of these materials vary significantly.

Payment Behaviour

Victims reported:

- Multiple payments in rapid succession
- Inconsistent amounts
- Unique UPI IDs in each complaint

The short extraction windows suggest that operators want to move funds quickly and discard mule accounts before they attract attention.

Communication Patterns

All complaints follow the same high-level structure:

- Polite introduction
- Reassurance
- A small initial payment
- Rapid escalation
- Pressure when questioned
- Sudden disappearance

The tone, pacing, and narrative differ across cases, indicating multiple operators.

Variation in Scam Depth

Some scammers stop after small attempts.
Others pursue extended extraction.
This reflects different operators with different levels of patience and risk tolerance.

Additional Pivots

Some complaints mentioned:

- The email: escortservicemalenational@gmail.com
- A related domain: gigoloclubindia.com

These appear rarely and cannot be linked conclusively.

Interpretation

The structure of the scam remains consistent, but the execution changes from operator to operator. This strongly supports the model of distributed scammers working independently from a shared entry point.

Operational Assessment

The Website as the Entry Point

The website directs victims into WhatsApp via the contact button.
This is where the scam begins and where all variation originates.

The Scam Flow

1. Initial reassurance and a small fee
2. Escalation through multiple fees
3. Tight time gaps between payments
4. Pressure when the victim resists
5. Abandonment once extraction ends

Distributed Extraction Model

Each operator uses:

- Different UPI accounts
- Different document templates
- Different conversational styles
- Different escalation strategies

This explains the lack of pattern consistency across complaints.

Cashout Behaviour

Mule accounts appear temporary and are likely abandoned quickly.
Extraction is fast and opportunistic.

Interpretation

The system remains resilient because:

- The attraction layer is centralised
- The extraction layer is decentralised
- No single operator's failure affects the domain

This structure makes attribution difficult and helps the operation continue despite complaints.

Intelligence Gaps

1. Attribution is blocked by WHOIS privacy and shared hosting.
2. Financial linkage between UPI accounts cannot be confirmed.
3. No cross-platform investigation was conducted.
4. The origins of edited documents remain unknown.
5. Relationships between operators cannot be established.
6. The size of the broader ecosystem is unclear.

These gaps reflect the chosen passive scope.

Conclusion

The available evidence indicates that indiangigoloclub.com operates as a long-running attractor site rather than the central point of the scam. Its role is to draw victims into contact with a rotating set of independent scammers who use unique mule accounts, improvised documents, and varied pressure tactics.

The consistency of the procedure and the inconsistency of the details point to a two-layer structure:

- The website’s role is to generate interest.
- Different operators perform the extraction.

This explains the scattered traces, varied scam depth, and absence of repeated financial identifiers. Within the limits of passive OSINT, this is the most coherent and supported assessment of the operation.