OSINT Investigation Report #2

Title: OSINT-Based Investigation of a High-Risk Online Investment Platform
Analyst: Shourya Kashyap
Date: January 2026

Section 1: Introduction

Project Title

OSINT-Based Investigation of an Online Investment Platform

Objective

The objective of this project is to analyse and verify the legitimacy of an online investment platform using open-source intelligence (OSINT) techniques. The investigation focuses on technical analysis, infrastructure assessment, document verification, and regulatory validation to identify potential fraud indicators.

Scope of Investigation

This investigation was limited to publicly available information and non-intrusive analysis methods, including application analysis, domain intelligence, metadata examination, and regulatory database verification. No direct interaction, exploitation, or unauthorized access was performed during the investigation.

Section 2: Methodology

The investigation was conducted using open-source intelligence (OSINT) techniques and static analysis methods. Only publicly accessible data and non-intrusive tools were used to ensure ethical and legal compliance throughout the research process.

The following methodologies were applied:

- Static analysis of the Android application using security analysis platforms
- Identification and analysis of associated domains and backend infrastructure
- Network and hosting intelligence correlation using OSINT tools
- Metadata analysis of certification and promotional materials
- Verification of regulatory and company registration claims through official government databases
- Digital footprint analysis to validate leadership identity claims

All findings were documented and cross-verified across multiple independent sources to ensure accuracy and reliability.

Section 3: Tools and Resources Used

The following tools and platforms were used during the investigation to collect and analyse open-source intelligence data:

- **VirusTotal** – for initial APK reputation and indicator identification
- **Mobile Security Framework (MobSF)** – for static Android application analysis
- **URLScan.io** – for website behaviour and network request analysis
- **Shodan** – for infrastructure and hosting intelligence
- **EXIFTool** – for metadata analysis of certification and promotional images
- **Wayback Machine** – for historical website footprint analysis
- **SEC EDGAR Database** – for verification of U.S. regulatory filings
- **ASIC Company Register** – for Australian company registration verification

All tools were used in read-only or passive analysis mode, without interacting with or modifying any external systems.

Section 4: Application Analysis Findings

Static analysis of the Android application revealed that the app does not function as a fully native trading platform. Instead, it operates primarily as a WebView-based container that dynamically loads content from external domains.

Key observations include:

- The application relies entirely on active internet connectivity to function
- Core logic and user interface elements are delivered remotely via web content
- No internal trading engine or transaction-processing logic was identified within the application
- The app structure is consistent with loader-style architectures commonly used to control behaviour from backend servers

These findings indicate that application behaviour can be modified server-side without requiring updates to the installed APK, significantly reducing transparency and increasing operational risk for users.

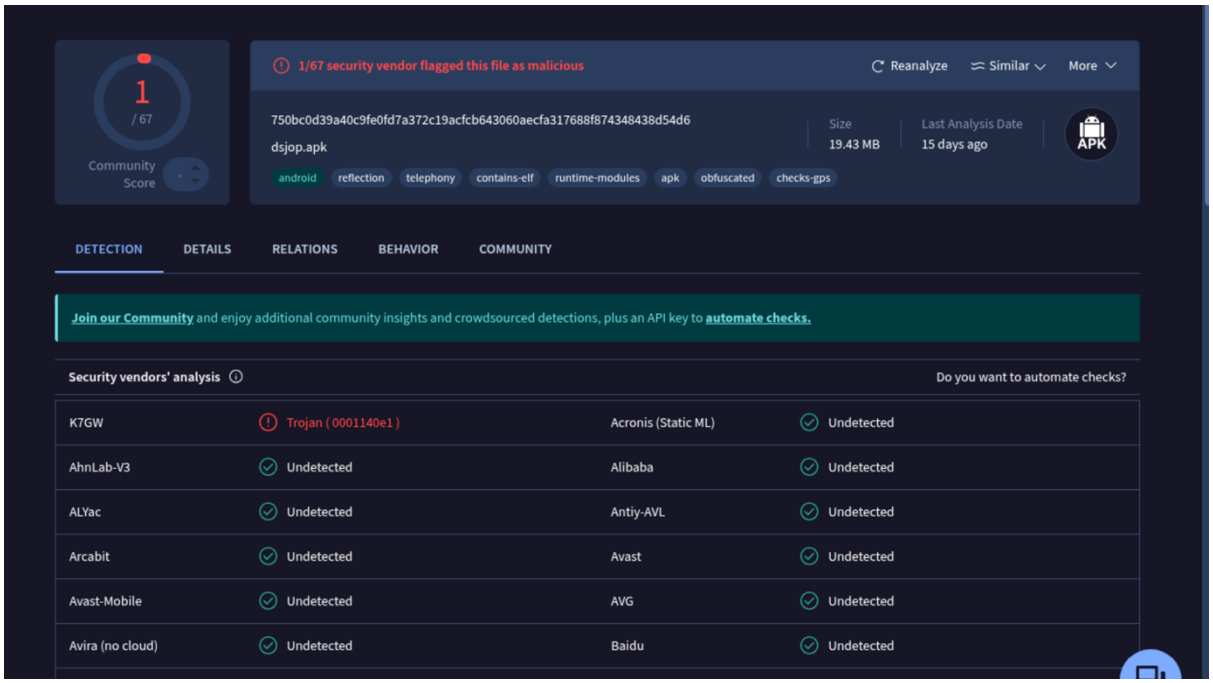
Section 5: Detailed Findings and Evidence

This section documents the key findings identified during the investigation, supported by screenshots and verifiable technical indicators.

5.1 Android Application Findings

- The analysed APK functions as a WebView-based application rather than a native trading platform.
- Core application behaviour is controlled by externally loaded web content.
- No internal trading logic or financial processing modules were identified.
- Application behaviour depends entirely on remote server responses.

Evidence:



File Name:	dsjop.apk
Package Name:	com.qkl.men0uv7q
Scan Date:	Jan. 20, 2026, 4:29 p.m.
App Security Score:	42/100 (MEDIUM RISK)

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	7	2	1	1

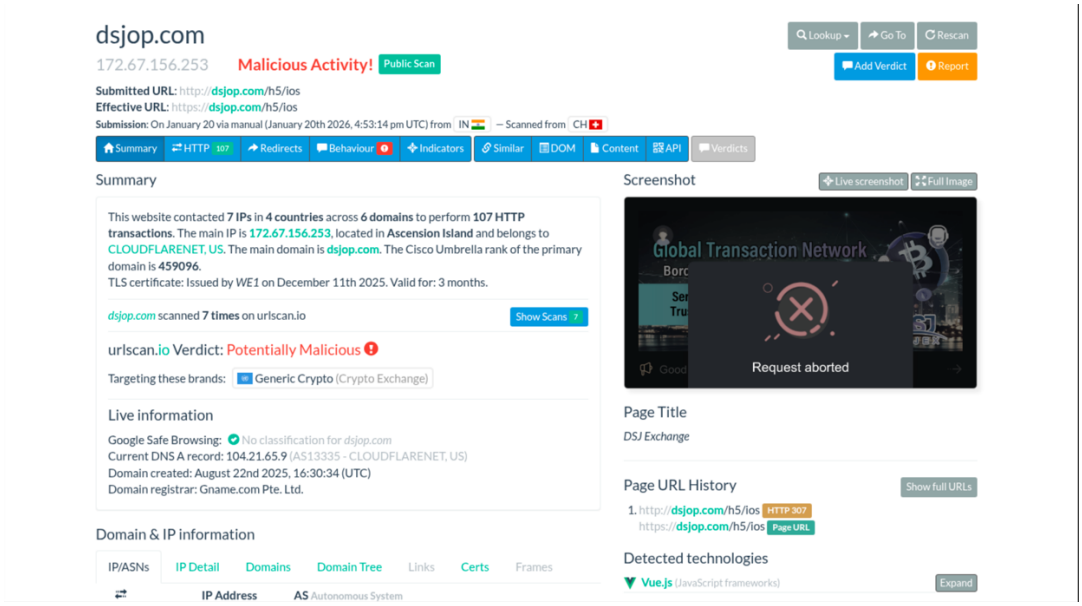
FILE INFORMATION

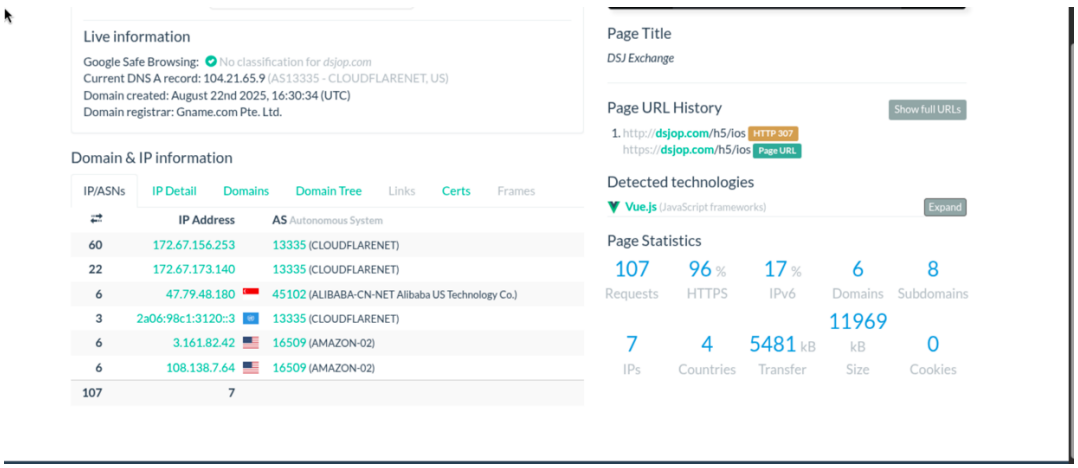
File Name: dsjop.apk
Size: 19.43MB
MD5: 92f01d49fc54de2a79e3e3a3c57f6a67
SHA1: ebb0743032ec3d33223cbb51212122bc64cc3a47
SHA256: 750bc0d39a40c9fe0fd7a372c19acfcb643060aecfa317688f874348438d54d6

5.2 Domain and Infrastructure Findings

- Multiple domains were identified operating as part of the same platform ecosystem.
- Domain behaviour analysis revealed centralized backend communication.
- Infrastructure analysis showed the use of CDN masking and cloud-hosted backend resources.

Evidence:





urlscan.io Home Search Live API Blog Memory usage: 120 MB SecurityTrails

dsj960.com

104.21.8.219 **Malicious Activity!** Public Scan

Lookup Go To Rescan Add Verdict Report

Submitted URL: http://dsj960.com/
Effective URL: https://dsj960.com/pc/
Submission: On January 20 via manual (January 20th 2026, 4:50:54 pm UTC) from IN — Scanned from CA

Summary HTTP 127 Redirects Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted **7 IPs** in **3 countries** across **7 domains** to perform **127 HTTP transactions**. The main IP is 104.21.8.219, located in **Ascension Island** and belongs to CLOUDFLARENET, US. The main domain is **dsj960.com**.
TLS certificate: Issued by *WE1* on December 11th 2025. Valid for: 3 months.

dsj960.com scanned **14 times** on urlscan.io Show Scans 14

urlscan.io Verdict: Potentially Malicious

Targeting these brands: Generic Crypto (Crypto Exchange)

Live information

Google Safe Browsing: No classification for *dsj960.com*
Current DNS A record: 188.114.96.3 (AS13335 - CLOUDFLARENET, US)
Domain created: August 22nd 2025, 17:22:04 (UTC)
Domain registrar: Gname.com Pte. Ltd.

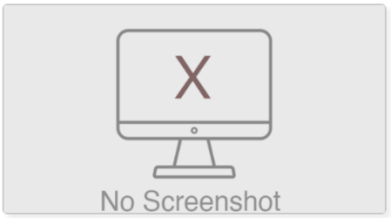
Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

	IP Address	AS Autonomous System
1 → 70	104.21.8.219	13335 (CLOUDFLARENET)
1	104.16.80.73	13335 (CLOUDFLARENET)
38	104.21.30.192	13335 (CLOUDFLARENET)
10	47.79.48.180	45102 (ALIBABA-CN-NET Alibaba US Technology Co.)
1	18.173.132.36	16509 (AMAZON-02)
1	104.21.58.74	13335 (CLOUDFLARENET)
127	7	

Screenshot

Live screenshot Full Image



Page Title

DSJ Exchange

Page URL History

Show full URLs

1. http://dsj960.com/ HTTP 307
   https://dsj960.com/ Page URL

Live information

Google Safe Browsing: No classification for *dsj960.com*
Current DNS A record: 188.114.96.3 (AS13335 - CLOUDFLARENET, US)
Domain created: August 22nd 2025, 17:22:04 (UTC)
Domain registrar: Gname.com Pte. Ltd.

Domain & IP information

Page Title

DSJ Exchange

Page URL History

Show full URLs

1. http://dsj960.com/ HTTP 307
   https://dsj960.com/ Page URL
2. https://dsj960.com/pc/index.html HTTP 307
   https://dsj960.com/pc/ Page URL

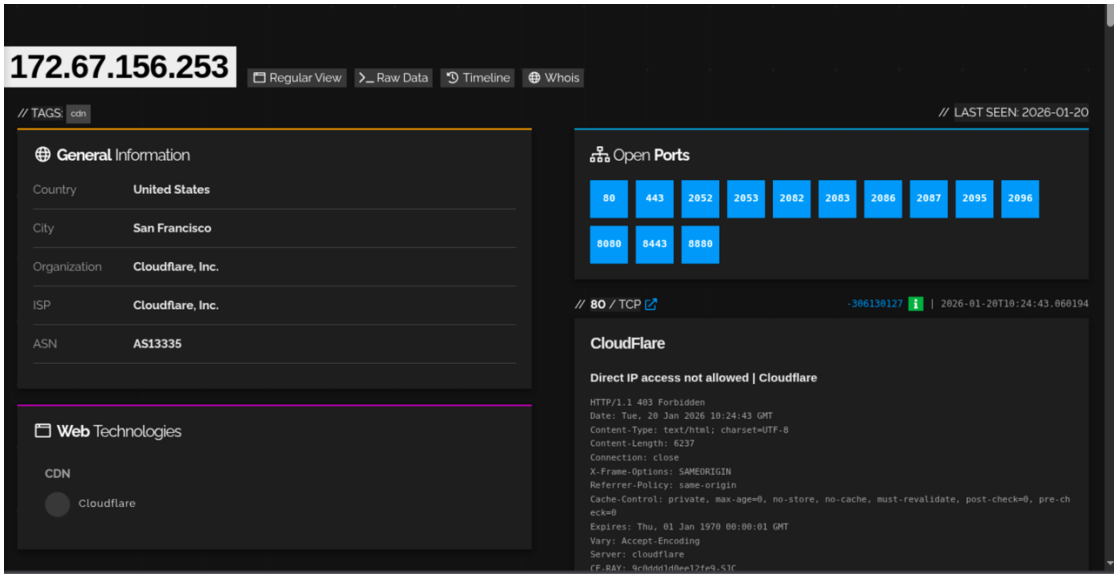
Detected technologies

dc.js (JavaScript graphics) Expand
Vue.js (JavaScript frameworks) Expand
Cloudflare Browser Insights (Analytics) Expand

Page Statistics

127	94 %	0 %	7	9
Requests	HTTPS	IPv6	Domains	Subdomains

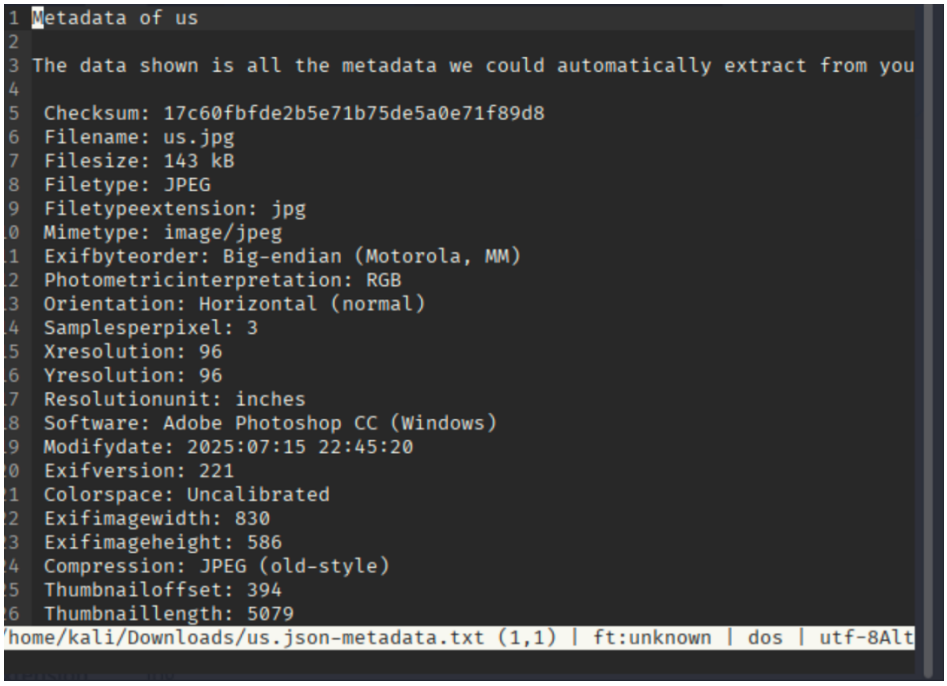
7	3	6788 kB	14101 kB	0
IPs	Countries	Transfer	Size	Cookies



5.3 Certification and Document Verification

- Multiple certifications displayed on the platform were analysed.
- Metadata examination confirmed that certification images were digitally created or edited using Adobe Photoshop.
- No official verification portals or issuing authority validation mechanisms were identified.

Evidence:

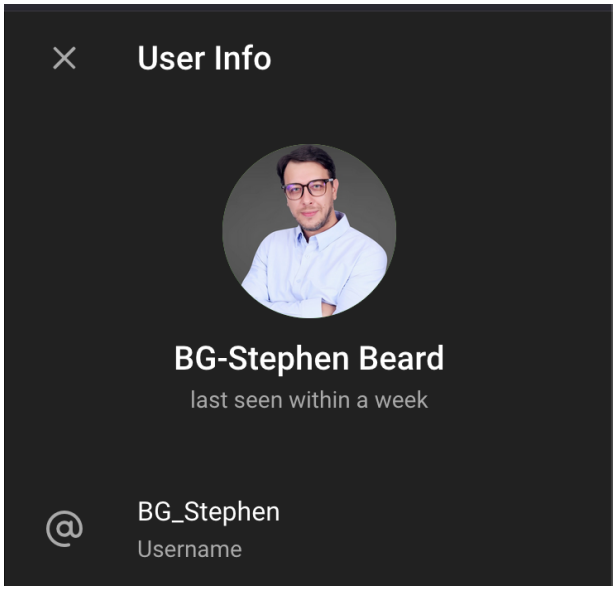


5.4 Leadership Identity Verification

- The individual presented as company leadership could not be independently verified through public professional records.
- No historical digital footprint, prior affiliations, or external references were identified beyond the company's own website.

NOTE
During recorded public video sessions, the individual presented as company leadership demonstrated noticeable inconsistencies between the claimed background and observable communication patterns. The individual's spoken English exhibited non-native fluency characteristics, including irregular pronunciation and scripted delivery. While this does not confirm identity or origin, it raises concerns when combined with the absence of independent professional verification.

Evidence:



5.5 Regulatory Verification Findings

- U.S. SEC filings were limited to Form D submissions, which are self-reported and explicitly unreviewed.
- Australian company registration was confirmed; however, no Australian Financial Services Licence (AFSL) was identified.
- Absence of required licensing indicates lack of authorization to provide trading or investment services.

Evidence:

- SEC EDGAR disclaimer screenshots
- ASIC registration records
- AFSL registry search results

Finding **0002076856** in D (Notice of sales of unregistered securities) of filed (2025-07-11) ‹ Previous 1 of 1 Next ›

The Securities and Exchange Commission has not necessarily reviewed the information in this filing and has not determined if it is accurate and complete.
The reader should not assume that the information is accurate and complete.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549
Intentional misstatements or omissions of fact constitute federal criminal violations. See 18 U.S.C. 1001.

OMB APPROVAL
OMB Number: 3235-0076
Estimated average burden hours per response: 4.00

FORM D

Notice of Exempt Offering of Securities

1. Issuer's Identity

CIK (Filer ID Number) | Previous [x] None | Entity Type

Open document | Open filing | Close

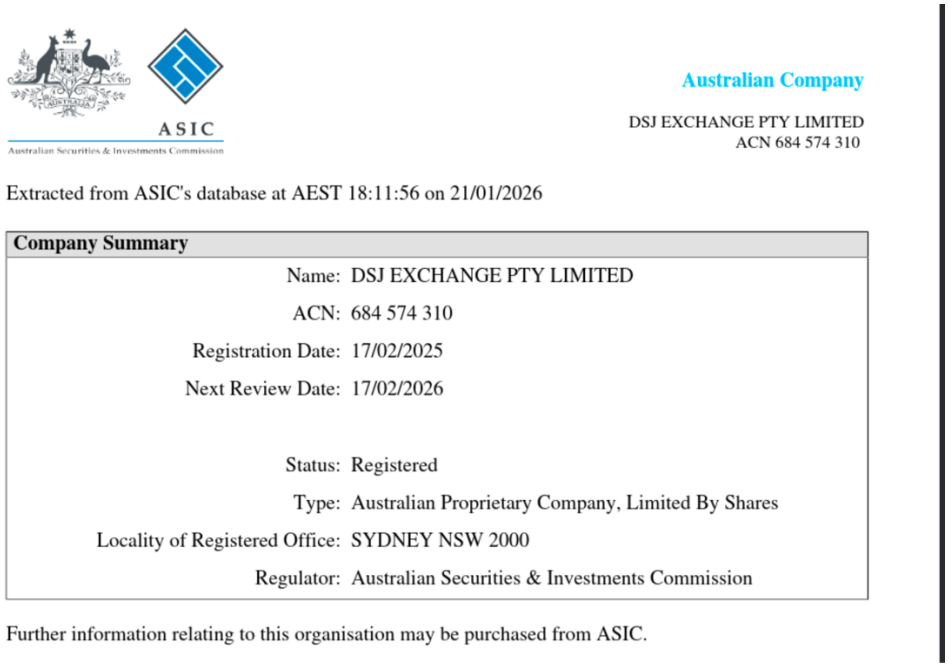
Name of Issuer
DSJ Exchange PTY Ltd

Street Address 1		Street Address 2	
3190 SOUTH VAUGHN WAY			
City	State/Province/Country	ZIP/PostalCode	Phone Number of Issuer
AURORA	COLORADO	80014	1-702-545-5691

3. Related Persons

Last Name	First Name	Middle Name
PARRAL	YERALDO Y	
Street Address 1	Street Address 2	
3190 South Vaughn Way		
City	State/Province/Country	ZIP/PostalCode
Aurora	COLORADO	80014

Relationship: [ ] Executive Officer [X] Director [ ] Promoter



ASIC
Australian Securities & Investments Commission

Australian Company

DSJ EXCHANGE PTY LIMITED
ACN 684 574 310

Extracted from ASIC's database at AEST 18:11:56 on 21/01/2026

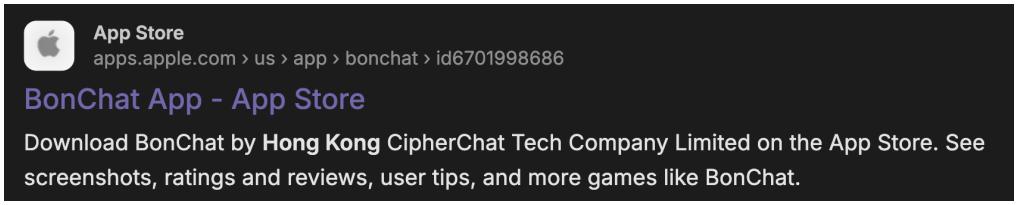
Company Summary

Name:	DSJ EXCHANGE PTY LIMITED
ACN:	684 574 310
Registration Date:	17/02/2025
Next Review Date:	17/02/2026
Status:	Registered
Type:	Australian Proprietary Company, Limited By Shares
Locality of Registered Office:	SYDNEY NSW 2000
Regulator:	Australian Securities & Investments Commission

Further information relating to this organisation may be purchased from ASIC.

5.6 Technology and Infrastructure Ecosystem Observations

The investigation identified that the platform relies on multiple third-party technologies and services originating from the East Asian technology ecosystem. These include cloud hosting, application dependencies, and communication platforms commonly used within that ecosystem. While the use of such technologies is not inherently malicious, the lack of transparency regarding infrastructure ownership, combined with offshore hosting and limited regulatory disclosures, increases operational opacity. This architectural design complicates accountability and traceability, particularly in financial service environments that typically require higher levels of regulatory oversight.



Section 6: Risk Assessment

Based on the findings obtained through application analysis, infrastructure investigation, document verification, identity validation, and regulatory review, the platform presents a **high-risk profile** for users.
The following risk factors were identified:

- **Regulatory Risk:**
  The entity lacks required financial service licensing (AFSL) necessary to legally provide trading or investment services.
- **Operational Risk:**
  Core platform functionality is controlled remotely through external web infrastructure, allowing unrestricted modification of user-facing behaviour.
- **Identity Risk:**
  Claimed leadership could not be independently verified through professional or historical digital records.
- **Documentation Risk:**
  Certifications displayed on the platform were identified as digitally created promotional materials without verifiable issuing authorities.
- **Transparency Risk:**
  Absence of publicly available audits, disclosures, or verifiable trading partners limits accountability.
- **Financial Risk:**
  The profit model and withdrawal structure are inconsistent with regulated trading environments and introduce elevated risk to user funds.

Considering the convergence of these factors, the platform demonstrates multiple indicators commonly associated with fraudulent or deceptive investment operations. Users interacting with such platforms face a significant likelihood of financial loss.

Section 7: Conclusion

This investigation applied open-source intelligence techniques to evaluate the legitimacy of an online investment platform. Through technical analysis, infrastructure assessment, document verification, identity validation, and regulatory review, multiple high-risk indicators were identified. The findings demonstrate a consistent pattern of operational opacity, unverifiable claims, absence of required financial licensing, and reliance on digitally fabricated promotional materials. No independently verifiable evidence was found to support the platform's claims of regulated trading operations or executive legitimacy.
While no intrusive testing or direct interaction was performed, the convergence of independent indicators strongly suggests that the platform does not meet the standards expected of a

legitimate or regulated financial service provider. Based on the totality of evidence, the platform presents a **high probability of fraud-related risk** to users.
This report is intended solely for educational, and awareness purposes and reflects analysis conducted using publicly available information.
