Created by: Gil Klainert FP NYC

Date: 2025-06-07

Investigation Risk Assessment Report

Investigation Summary

Investigation ID:	INV-All-TESTS
User ID:	4621097846089147992
Time Range:	60d
Overall Risk Score:	0.88
Status:	Unknown
Generated:	2025-06-07 00:50:26

Module Analysis Summary

Module	Risk Score	Records	Status
Device Analysis	0.85	23	High Risk
Location Analysis	0.90	23	High Risk
Network Analysis	0.80	23	High Risk
Logs Analysis	0.70	1	High Risk

Detailed Module Analysis

Device Analysis (Risk Score: 0.85)

Risk Level: HIGH RISK

Records Analyzed: 23

Analysis:

The signals indicate overlapping timeframes in Mountain View (US) and Bengaluru (IN) from separate device IDs. These short time intervals strongly suggest impossible or near-impossible travel, implying either a VPN/proxy, shared account usage, or a compromised account. The frequency of device changes underlines the suspicious nature of this activity.

Key Risk Factors:

• Multiple device IDs from distinct countries (US and India)

• Rapid switching indicating possible account sharing or compromised credentials

Location Analysis (Risk Score: 0.90)

Risk Level: HIGH RISK

Records Analyzed: 23

Analysis:

Official OII data shows the user’s address is in San Diego, CA (USA). However, logs reveal multiple sign-ins from Bengaluru, India (f394742f39214c908476c01623bf4bcd) very close in time to sign-ins from Mountain View, US (e9e49d25e6734402a32f797e55d98cd9 and 392b4bf1e3ed430090a9f50f1d72563a). This pattern indicates likely impossible travel or proxy-based location masking. The vector search analysis shows consistent similar records (distance=8), yet the key anomaly is the abrupt change of countries, conflicting with the official address (USA). This geographic mismatch strongly suggests suspicious usage, potential account sharing, or compromise.

Key Risk Factors:

- Device usage from India (IN) while official address is USA
- Multiple devices accessing account from US and IN in short timespan
- Impossible travel timeframe between California (US) and Bengaluru (IN)

Network Analysis (Risk Score: 0.80)

Risk Level: HIGH RISK

Records Analyzed: 23

Analysis:

The user’s network signals indicate a quick transition between a US-based ISP and an India-based ISP, which is suspicious given the short timeframe. Such behavior may reflect account sharing, compromised credentials, or IP masking. The repeated pattern of sudden ISP changes heightens the risk.

Key Risk Factors:

- Multiple IPs in a short timeframe
- Rapid shift from US-based ISP to India-based ISP

Logs Analysis (Risk Score: 0.70)

Risk Level: HIGH RISK

Records Analyzed: 1

Analysis:

Medium risk. The user had at least one failed password attempt and logins from diverse locations, indicating possible suspicious activity.

Key Risk Factors:

- One failed password attempt (challenge_failed_incorrect_password)
- Multiple IPs from geographically distinct regions

Overall Risk Assessment

Final Risk Score: 0.88 (HIGH RISK)

Final Assessment:

The user’s activities demonstrate several strong indicators of elevated fraud risk based on multiple points of evidence. First, there is clear device-based evidence of overlapping usage in Mountain View (US) and Bengaluru (IN) within short time windows. This quick switch between two far-apart regions suggests either impossible travel or the

use of proxy services. The fast-paced transitions and multiple device fingerprints strengthen the suspicion of account sharing or compromise.

Location data further corroborates these concerns because the user’s official address is listed in San Diego, California, yet repeated logins appear to originate from India. This stark mismatch between official location and actual usage points to possible identity misuse, unauthorized account access, or the deliberate masking of true whereabouts.

From the network perspective, the rapid ISP changes—switching almost immediately from a US-based ISP to an India-based ISP—indicate significant geographic jumps in a very short timeframe. Such abrupt shifts are frequently associated with suspicious or fraudulent behavior, including credential theft, use of VPNs, or automated account access. The limited log data does not contradict these concerns but also does not provide additional reassurance.

Taken in totality, these anomalies support a high degree of risk. The combination of repeated sign-ins from multiple countries conflicting with the official address in the United States, compressed timeframes that make legitimate travel implausible, and the potential use of proxy or VPN technology all point toward the user’s activity being very likely fraudulent. Accordingly, the risk score for the user is 0.88, indicating a need for immediate scrutiny. Recommended next steps include tightening authentication measures (e.g., multifactor authentication), verifying user identity through additional channels, and closely monitoring subsequent login attempts for any further abnormal geographic or network patterns.