Created by: Gil Klainert FP NYC

Date: 2025-06-11

Investigation Risk Assessment Report

Investigation Summary

Investigation ID:	INV-All-TESTS
Entity ID:	4621097846089147992
Entity Type:	user_id
Time Range:	120d
Overall Risk Score:	0.05
Status:	Unknown
Generated:	2025-06-11 10:20:44

Module Analysis Summary

Module	Risk Score	Records	Status
Device Analysis	0.00	0	Low Risk
Location Analysis	0.00	0	Low Risk
Network Analysis	0.00	0	Low Risk
Logs Analysis	0.00	0	Low Risk

Detailed Module Analysis

Device Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:
No detailed analysis available for this module.

Location Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

No device location data is available, so no anomalies can be detected. The user's official address is in the USA (California), and there are no recorded device locations that differ from the official address.

Network Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

Since no data is available for analysis, there is no basis to identify potential device or geographic anomalies. The risk is minimal by default and the confidence is very low due to insufficient evidence.

Logs Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

LLM invocation/validation error: LLM invocation/validation error: No authentication logs found for this user.

Key Risk Factors:

• LLM invocation/validation error: LLM invocation/validation error: No authentication logs found for this user.

Overall Risk Assessment

Final Risk Score: 0.05 (LOW RISK)

Final Assessment:

Based on the absence of device, location, network, or logs data, we have insufficient indications of any suspicious behavior. Without reliable data or evidence of unusual activity, there is understandably minimal basis for concern. Therefore, the risk score for the user is low by default, but with a limited data set, we cannot conclusively rule out potential risks that remain undetected. This limited visibility reduces our confidence level and warrants cautious interpretation.

In reviewing the signals assessed so far, there are no clear signs of malicious device usage, suspicious travel patterns, proxy or VPN usage, nor any anomalies in network usage. However, these conclusions are based on minimal or nonexistent underlying data, which means the overall picture could be incomplete. The risk score for the user reflects the current findings of minimal identified threats, but the lack of corroborating evidence leaves open the possibility that certain risks—albeit unlikely—remain hidden.

Given these circumstances, we recommend collecting additional, higher-quality data points to increase confidence in this assessment. If feasible, gathering device logs, location data, and network metrics would provide further clarity. In the meantime, continued monitoring, along with standard security practices such as user authentication checks and proactive fraud detection measures, should be maintained. Until more data becomes available, the risk score for the user stands at a cautiously low level, and further investigation may be warranted if new information emerges.