Created by: Gil Klainert FP NYC

Date: 2025-06-09

# Investigation Risk Assessment Report

## Investigation Summary

| | |
|---|---|
| Investigation ID: | INV-All-TESTS |
| User ID: | 4621097846089147992 |
| Time Range: | 120d |
| Overall Risk Score: | 0.20 |
| Status: | Unknown |
| Generated: | 2025-06-09 11:58:48 |

## Module Analysis Summary

| Module | Risk Score | Records | Status |
|---|---|---|---|
| Device Analysis | 0.20 | 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: 0.20)

Risk Level: LOW RISK

Records Analyzed: 0

Analysis:

With no device signals, there are no identifiable geographic or device anomalies. Therefore, the risk assessment defaults to low risk.

### Location Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

### Analysis:

No anomalies detected due to absence of any device location data; all known addresses match the official country (USA).

## Network Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

### Analysis:

No LLM assessment due to LLM invocation/validation error.

### Key Risk Factors:

- LLM invocation/validation error: Error code: 424 - {'error_message': 'External service dependency could not finish in time',

## Logs Analysis (Risk Score: 0.00)

Risk Level: LOW RISK

Records Analyzed: 0

### Analysis:

No authentication logs found for this user.

### Key Risk Factors:

- No logins found

## Overall Risk Assessment

### Final Risk Score: 0.20 (LOW RISK)

### Final Assessment:

Based on the available information, the user shows minimal indications of anomalous activity. Specifically, there are no identified discrepancies between the user’s officially recorded address and the current location data, which suggests that the user’s behavior is largely consistent with their known information. Additionally, there are no concerning device-related signals nor network indicators of suspicious activity.

While the absence of detailed device and network telemetry constrains the depth of our assessment, what has been provided so far does not raise any obvious red flags beyond a minimal advisory note that certain data sources are incomplete. Taken together, these observations led us to compute a risk score for the user of 0.2, reflecting a low overall likelihood of fraudulent or high-risk behavior.

As a recommended next step, more thorough device logs or stronger location data could confirm the legitimacy of transactions and general user activity. Monitoring for any unusual network patterns or sudden changes in device usage is also advisable. If available, cross-checking additional telemetry concerning login frequency and geolocation trends may further validate the current low-risk conclusion.

In summary, while there are areas where more data would offer added certainty, the current analysis supports the overall conclusion that the user poses a generally low risk. However, continued vigilance and ongoing monitoring remain important measures to ensure protective safeguards against emerging threats.

Report generated on 2025-06-09 at 11:59:09