**Mock AI Use Case Risk Assessment**

FraudGuard

# Description of the AI use case

FraudGuard is an AI-powered fraud detection system that analyzes financial transactions in real-time. It uses machine learning models to identify unusual spending patterns, anomalies, and suspicious behaviors to prevent fraudulent activities. The system is deployed within banking environments and integrates with payment platforms to automatically flag or block high-risk transactions.

# Risk identification

**EB-02 – Ethical and Bias: Bias in Fraud Detection**

FraudGuard may disproportionately flag certain demographic groups or regions as 'high-risk' due to biased training data, leading to unfair treatment of legitimate customers.

**SP-02 – Security and Privacy: PII Exposure**

As FraudGuard processes sensitive financial and personal data, adversaries may exploit vulnerabilities, resulting in data breaches or misuse of Personally Identifiable Information (PII).

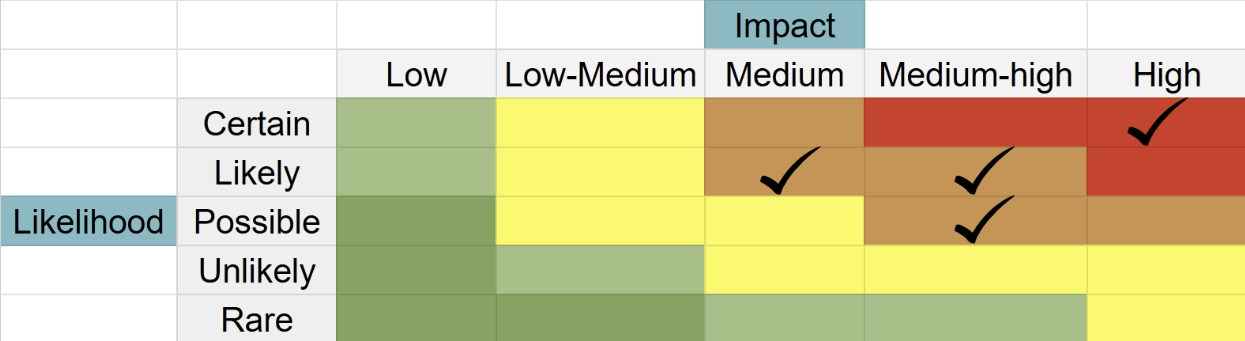
**OT-02 – Operational and Technical: Model Drift**

Over time, fraud patterns change. If FraudGuard is not retrained, it may lose accuracy, leading to missed fraud or false positives that inconvenience customers.

**RR-02 – Regulatory and Reputational: Regulatory Non-Compliance**

Failure to comply with financial regulations (e.g., GDPR, PCI DSS, EU AI Act) could result in fines, sanctions, or reputational damage.

# Impact vs Likelihood scoring



Using the provided heatmap scale (Rare → Certain, Low → High), the risks are scored as follows:

**EB-02 – Bias in Fraud Detection:** Likelihood = Possible, Impact = Medium-high

**SP-02 – PII Exposure:** Likelihood = Unlikely, Impact = High

**OT-02 – Model Drift:** Likelihood = Likely, Impact = Medium

**RR-02 – Regulatory Non-Compliance:** Likelihood = Possible, Impact = High

# Overall risk rating

**EB-02 – Bias in Fraud Detection:** High

**SP-02 – PII Exposure:** High

**OT-02 – Model Drift:** Medium

**RR-02 – Regulatory Non-Compliance:** Critical

# Suggested controls/mitigations

**EBC-02 – Ethical and Bias: Diverse training datasets**

Ensure diverse and representative training data to reduce demographic bias.

**SPC-01 – Security and Privacy: Data encryption & access control**

Encrypt sensitive customer data and enforce role-based access to prevent unauthorized exposure.

**OTC-01 – Operational and Technical: Model retraining & drift monitoring**

Regularly retrain FraudGuard on updated fraud datasets and set automated drift alerts.

**RRC-01 – Regulatory and Reputational: Regulatory compliance program**

Conduct periodic audits, maintain compliance documentation, and align with GDPR, PCI DSS, and EU AI Act requirements.

# Summary

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Category** | **Risk Name** | **Likelihood** | **Impact** | **Overall Rating** |
| EB-02 | Ethical and Bias | Bias in Fraud Detection | Possible | Medium-High | High |
| SP-02 | Security and Privacy | PII Exposure | Unlikely | High | High |
| OT-02 | Operational and Technical | Model Drift | Likely | Medium | Critical |

**END**