

Fraud Detection Policy

Objective

Detect and mitigate application fraud using model-driven risk indicators derived from SVM model outputs.

Scope

Applies to all new credit and card applications processed by the institution.

Positive Fraud Signals (Risk Increasing)

1. Missing Previous Address Duration: If the number of months in the previous registered address is missing, this is considered a strong fraud signal. 2. Device Operating System = Windows: Applications submitted from Windows devices are considered a moderate fraud signal.

Negative Fraud Signals (Risk Reducing)

1. Session Persistence on Logout: User keeping session alive is a negative fraud indicator. 2. Name–Email Similarity: High similarity between applicant name and email handle reduces fraud likelihood. 3. Valid Home Phone Number: Validated home phone numbers reduce fraud risk. 4. Existing Cards with Same Banking Company: Existing customer relationship is a strong negative fraud signal. 5. Housing Status (BE, BB, BC): These anonymized categories are historically associated with lower fraud rates.

Escalation Rules

Manual review is required if: • Missing previous address duration AND Windows OS • Missing previous address duration with no negative signals • Two or more strong positive indicators Auto-approval may proceed if: • No positive signals and at least two strong negative signals • Existing validated customer with strong identity indicators

Governance and Monitoring

• Risk thresholds reviewed quarterly • Model drift and bias monitoring conducted regularly • Signals treated as probabilistic, not deterministic proof of fraud

Risk Impact Summary

Signal	Direction	Strength
Missing Previous Address	Increase Risk	Strong
Windows OS	Increase Risk	Moderate
Session Persistence	Reduce Risk	Moderate
Name–Email Similarity	Reduce Risk	Moderate
Valid Home Phone	Reduce Risk	Moderate
Existing Cards with Bank	Reduce Risk	Strong
Housing Status BE/BB/BC	Reduce Risk	Low–Moderate