

CyberAntifraud Model Card Template

Audit ready documentation for fraud models in acquiring

Purpose

Provide a standardized model card that enables auditability, reviewer clarity, and operational traceability.

This template is intended for each model release and major retraining.

Model overview

Model name, version, date, owner, intended use, and out of scope use cases.

Target label definition, decision type, and criticality classification.

Data

Training window, validation windowing, data sources, sampling, and preprocessing steps.

PII handling, minimization choices, and any synthetic or anonymized transformations.

Evaluation

Temporal backtests summary across rolling windows. Primary metrics and dispersion.

Cost assumptions, threshold policy, and operational constraint checks.

Fairness and bias

Document any bias tests performed, proxy variables considered, and mitigation steps if needed.

Explain limitations. Avoid claiming fairness guarantees without evidence.

Drift and monitoring

Define drift indicators, calibration monitoring, data quality checks, and canary tests.

Define retraining triggers and rollback criteria.

Governance and sign off

Approvals, change log, links to experiment tracking, and evidence artifacts.

Incident response plan if unexpected behavior is detected in production.