**Fraud Monitoring Plan for LexisNexis InstantID**

**1. Objective**

This document defines the monitoring framework for LexisNexis InstantID in a third-party offshore validation context where direct access to personally identifiable information (PII) is restricted. The objective is to validate model stability, fraud capture performance, and business outcomes using **non-PII, aggregated, and anonymized data**.

**2. Background**

LexisNexis InstantID is an identity verification engine used by the bank during customer onboarding. It checks submitted applicant details against external and internal databases and returns:

* A **Pass/Fail** or **Match/No Match** result for identity validation
* **Risk flags** (e.g., deceased person, SSN mismatch)
* A record of whether the bank **proceeded to approve or decline** the applicant

**3. Monitoring Areas**

| **Monitoring Area** | **Objective** |
| --- | --- |
| Verification Pass Rate | Track success rate of InstantID verification results (Pass vs Fail). |
| Alert Distribution Trends | Assess frequency of different risk flags (coded format) across time. |
| Override Analysis | Identify how often and under what flags overrides were made by the bank. |
| Identity Fraud Capture Rate | Evaluate how well InstantID flags correlated with future confirmed identity fraud. |
| False Decline Rate | Determine the rate at which InstantID flagged applicants who were actually good. |
| Stability (PSI on Match Categories) | Detect shifts in verification result types over time. |

**4. Data Requirements**

| **Field Name** | **Business Explanation** | **Metrics Supported** |
| --- | --- | --- |
| Application ID (Hashed) | Unique reference used for joining across results and fraud outcome tables | All metrics |
| Application Date | To group metrics monthly/quarterly | Trend, PSI, fraud timeline |
| Verification Result Code | Coded field (e.g., PASS, FAIL, REFER) | Verification Pass Rate, PSI, Alert Rate |
| Risk Flag Codes | Coded flags (e.g., F1 = SSN mismatch, F2 = Deceased) | Risk Distribution, Override Impact |
| Final Decision Code | Whether bank approved the account | False Decline Rate, Override Rate |
| Override Indicator | Whether bank overrode InstantID result | Override monitoring |
| Fraud Flag | Whether identity fraud occurred (provided post-facto by bank) | Fraud Capture, Miss Rate |
| Segment (Customer Type) | High-level segment (e.g., Student, Salaried, NRI – no raw identifiers) | Segment-wise fraud or flag trends |
| Channel Code | Origination channel: Online / Branch / Assisted | Channel-wise match/flag/fraud analysis |

**5. Key Metrics and Formulas**

| **Metric** | **Formula** | **Expected Range** |
| --- | --- | --- |
| **Verification Pass Rate** | Passed Verifications / Total Applications | > 85% |
| **Risk Flag Rate** | Applications with One or More Flags / Total Applications | Track trend |
| **Override Rate** | Overridden Failed Verifications / Total Failed Verifications | < 30% (watchlist) |
| **Fraud Capture Rate** | Flagged Applicants Who Became Fraud / Total Identity Frauds Identified | > 75% |
| **False Decline Rate** | Legitimate Customers Flagged by InstantID / Total Legitimate Applicants | < 3% |
| **PSI on Result Codes** | Σ (Mon% - Dev%) × ln(Mon% / Dev%) for Match Categories | < 0.10 (Stable) |





**Governance and Reporting**

* **Frequency**: Monthly tracking; quarterly deep dive
* **Owner**: Fraud Strategy / Risk Analytics / Validation Team
* **Red Flags**:
  + Match Rate drops > 5% over two months
  + PSI > 0.10 for any result code category
  + Fraud Capture Rate < 70%
* **Reporting Cadence**: Metrics provided to Model Risk Governance forum