**1. Background**

EWB has deployed **iProov Genuine Presence Assurance®** technology to enable secure, real-time biometric verification of customers during first-time digital onboarding.

iProov’s solution ensures that customer identity is authenticated accurately without requiring physical branch visits, reducing fraud risks such as impersonation and synthetic identity attacks.

Given the critical role digital onboarding plays in customer acquisition, fraud prevention, and regulatory compliance (KYC/AML), it is essential to continuously monitor iProov’s performance.  
This Monitoring Plan defines the approach, key metrics, data requirements, governance responsibilities, exception thresholds, and sample reporting framework to ensure operational robustness and risk management.

**2. Objective**

The objectives of this Monitoring Plan are to:

* Ensure **effective and reliable performance** of iProov authentication during onboarding.
* Detect **early warning signs of technical or operational issues**.
* Monitor **fraud leakage and customer drop-off risks**.
* Support **regulatory and internal model governance** expectations.

**3. Scope**

This Monitoring Plan covers:

* Use of **iProov during first-time digital onboarding of customers** through EWB’s mobile and web platforms.
* **Excludes** usage for high-risk transaction authentication or KYC refreshes.

**4. Key Metrics Monitored**

| **Metric** | **Definition** | **Business Importance** |
| --- | --- | --- |
| Authentication Success Rate | % of customers successfully authenticated. | Measures onboarding effectiveness and customer satisfaction. |
| Authentication Failure Rate | % of customers who fail authentication. | Indicates friction and possible experience issues. |
| False Rejection Rate (FRR) | % of genuine customers wrongly rejected. | Impacts customer acquisition and satisfaction. |
| False Acceptance Rate (FAR) | % of fraudulent users wrongly authenticated. | Measures fraud risk exposure. |
| Manual Review Rate | % of authentications needing human review. | Impacts operational load and efficiency. |
| Average Authentication Time (Latency) | Average time to complete authentication. | Impacts customer experience and app abandonment risk. |
| Service Availability | % uptime of iProov service. | System reliability and business continuity metric. |
| Fallback Rate | % of customers routed to alternative verification. | Indicates resilience but also possible friction points. |
| iProov Load Success Rate | % of customers where iProov module loaded successfully. | Measures app readiness and front-end stability. |

**5. List of Variables Required (Transaction-Level Raw Data)**

| **Variable Name** | **Business Explanation** | **Metric Supported** |
| --- | --- | --- |
| Transaction ID | Unique technical ID for each authentication attempt (masked). | To track and aggregate attempts. |
| Authentication Attempt Timestamp | Date and time of attempt. | To aggregate metrics weekly/monthly. |
| Authentication Outcome | Result per attempt (Success / Failure / Manual Review / Fallback). | Base for success, failure, manual, fallback calculations. |
| Fraud Confirmation Tag (optional) | Whether a successful authentication was later identified as fraudulent. | False Acceptance Rate. |
| False Rejection Tag (optional) | Whether a failed authentication was later verified as genuine. | False Rejection Rate. |
| Authentication Time (Seconds) | Duration from initiation to decision. | Average authentication latency. |
| Downtime/Error Code | Captures system-side errors/failures. | Service downtime tracking. |
| iProov Load Event Indicator | Captures whether iProov SDK loaded successfully on user device. | Load Success Rate monitoring. |

**Note:** No customer PII is required for monitoring purposes.

**6. Exception Thresholds**

| **Metric** | **Threshold** | **Action on Breach** |
| --- | --- | --- |
| Authentication Success Rate | < 95% | Investigate customer journey and technical stability. |
| False Rejection Rate | > 3% | Review liveness conditions, UX issues, lighting/environment issues. |
| False Acceptance Rate | > 0.5% | Escalate immediately to Fraud Risk for deeper review. |
| Authentication Latency | > 10 seconds | Investigate network/app performance bottlenecks. |
| Service Availability | < 99.9% uptime | Raise incident with vendor/vendor management escalation. |
| Manual Review Rate | > 5% | Review threshold settings with fraud operations. |
| Fallback Rate | > 2% | Analyze fallback triggers and alternate flows. |
| iProov Load Success Rate | < 98% | Review mobile/web app SDK integration health. |

**7. Monitoring Frequency**

| **Activity** | **Frequency** |
| --- | --- |
| Metric Tracking | Monthly |
| Exception Reporting | As breaches occur |
| Annual Monitoring Plan Review | Annually |

**8. Governance Structure**

| **Role** | **Responsibility** |
| --- | --- |
| Fraud Risk Management | Overall owner of fraud-related metrics and breaches. |
| Digital Banking Operations | Monitoring authentication journey performance. |
| Vendor Management | Overseeing iProov SLA compliance and issue escalation. |
| Model Risk Management | Governance oversight and periodic plan validation. |
| IT Operations | Tracking uptime, downtime, and integration issues. |

**9. Data Handling and Privacy**

* Only technical, non-PII transaction fields will be used for monitoring purposes.
* Monitoring dataset must comply with internal data privacy policies and applicable regulations (GDPR, CCPA).

**10. Sample Metric Calculation and Interpretation of Red/Amber Points**

**10.1 Sample Weekly Metric Calculation (Illustrative)**

| **Week** | **Total Attempts** | **Successful Auth** | **Failed Auth** | **False Rejects** | **False Accepts** | **Manual Reviews** | **Avg Time (s)** | **Downtime (mins)** | **Fallback Cases** | **Load Failures** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Week 1 | 1000 | 960 | 40 | 25 | 3 | 30 | 7.5 | 5 | 15 | 10 |

**Metric Calculations:**

* Authentication Success Rate = (960/1000) × 100 = **96.0%** ✅
* Authentication Failure Rate = (40/1000) × 100 = **4.0%**
* False Rejection Rate = (25/1000) × 100 = **2.5%** ✅
* False Acceptance Rate = (3/1000) × 100 = **0.3%** ✅
* Manual Review Rate = (30/1000) × 100 = **3.0%**
* Average Authentication Time = **7.5 seconds**
* Service Availability = (10080-5)/10080 × 100 ≈ **99.95%** ✅
* Fallback Rate = (15/1000) × 100 = **1.5%**
* iProov Load Success Rate = ((1000-10)/1000) × 100 = **99.0%** ✅

**10.2 Interpretation of Red and Amber Points**

| **Status** | **Interpretation** | **Example** |
| --- | --- | --- |
| 🟢 **Green** | Metric within acceptable threshold. | Authentication Success Rate = 96% (threshold = 95%). |
| 🟠 **Amber** | Metric nearing threshold, requires close monitoring. | Manual Review Rate = 4.9% (threshold = 5%). |
| 🔴 **Red** | Metric breached threshold, immediate investigation needed. | Avg Authentication Time = 11.5s (threshold = 10s). |

**📎 Annexure 1: Full Synthetic Data (10 Weeks)**

| **Week** | **Total Attempts** | **Successful Auth** | **Failed Auth** | **False Rejects** | **False Accepts** | **Manual Reviews** | **Avg Time (s)** | **Downtime (mins)** | **Fallbacks** | **Load Failures** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Week 1 | 1000 | 960 | 40 | 25 | 3 | 30 | 7.5 | 5 | 15 | 10 |
| Week 2 | 1050 | 990 | 60 | 20 | 2 | 28 | 8.0 | 10 | 18 | 5 |
| Week 3 | 950 | 910 | 40 | 30 | 5 | 35 | 9.0 | 12 | 22 | 12 |
| Week 4 | 980 | 920 | 60 | 32 | 1 | 40 | 11.5 🔴 | 7 | 25 | 15 |
| Week 5 | 1020 | 970 | 50 | 15 | 2 | 30 | 7.0 | 4 | 12 | 8 |
| Week 6 | 1100 | 1060 | 40 | 20 | 2 | 25 | 8.5 | 3 | 10 | 3 |
| Week 7 | 1000 | 920 | 80 | 50 | 8 | 55 🔴 | 8.0 | 15 | 30 | 10 |
| Week 8 | 990 | 970 | 20 | 10 | 1 | 20 | 6.5 | 2 | 8 | 4 |
| Week 9 | 1030 | 990 | 40 | 15 | 2 | 25 | 8.0 | 6 | 18 | 6 |
| Week 10 | 970 | 910 | 60 | 35 | 4 | 50 | 9.5 | 20 🔴 | 35 🔴 | 20 🔴 |