Non-Resident Bank Account Risk Management Protocol

This document proposes a global AML/KYC protocol for managing non-resident bank accounts.
The aim is to mitigate money laundering risks while allowing legitimate access to financial services.

1. Identification at Account Opening:
- Collect valid passport (primary ID).
- Collect secondary government-issued ID if available.
- Verify immigration entry stamp/eVisa (purpose of visit, duration).
- Introduce a special machine-readable verification stamp by immigration authorities.
  This confirms passport validity and purpose of visit. Only stamped passports are accepted.

2. Account Type & Limits:
- Visitor Accounts (short-term):
  * Deposit/balance limit (e.g., USD 10,000).
  * Restricted to basic services (no business accounts, limited transfers).
  * Auto-close on visa expiry unless upgraded.
- Resident Non-Citizen Accounts:
  * Medium risk categorization.
  * Upgrades to business products only after Enhanced Due Diligence (EDD)
    and confirmation from legislative/immigration authorities.

3. Real-Time Immigration Verification:
- Banks integrate with immigration systems using secure APIs.
- Bank verifies passport status digitally before opening accounts.
- Expired, overstayed, or flagged status results in rejection.

4. Ongoing Monitoring:
- Automated alerts for suspicious transactions.
- Restrict large international transfers unless source of funds is proven.
- Periodic account reviews (6 months for visitors, 12 months for residents).

5. Benefits:
- Reduces abuse of non-resident accounts for layering.
- Enhances AML by linking immigration data with banking data.
- Improves risk scoring accuracy and strengthens KYC standards.

This framework aligns with FATF objectives for digital KYC, risk-based approach, and closing regulatory loopholes for non-resident accounts.

Author: Elite AML Specialist Candidate