AI-Powered AML Detection Module – PRD

1. Module Overview

The Bank Statement Analyzer is an AI-driven module designed to automate parsing and analysis of financial statements for AML and fraud detection. It uses machine learning and OCR to extract transactions from PDFs or spreadsheets, then applies anomaly-detection algorithms and rule-based checks. The module provides visual analytics (e.g. link/network graphs and summary dashboards) to highlight complex money flows and suspicious patterns. For example, modern solutions claim “AI to instantly detect fraudulent documents, tampering attempts, and suspicious patterns” in statements. Visual link analysis simplifies uncovering hidden networks: by graphing accounts and flows, investigators can spot circular or round-trip transactions that would be hard to see in raw data. Overall, this module accelerates AML reviews by automating data extraction and surfacing red flags, enabling law enforcement and banking analysts to focus on high-risk cases quickly.

2. User Workflows

- **Single Statement Upload:** A user (investigator or compliance officer) uploads one statement (PDF, CSV, or Excel). The system OCR-extracts data, verifies PDF authenticity, and generates a report. The user sees metrics (balances, totals) and flagged transactions (e.g. large cash deposits, high-risk counterparty).

- **Multiple Statements (Same Bank & Individual):** The user uploads all statements for one account-holder at a single bank. The module consolidates transactions chronologically, computes aggregate metrics, and identifies internal flow irregularities (e.g. repeated withdrawals/deposits). Cross-link analysis within these statements highlights patterns like structuring or cyclical transfers.

- **Multiple Statements (Different Banks, Same Individual):** The user provides statements from several banks for one person. The system unifies data (using customer identifiers) and correlates transactions across banks. This reveals inter-bank transfers and cash routing, enabling detection of schemes like “round-robin” transfers between the person’s accounts. It also calculates overall transaction summaries for the individual.

- **Statements (Different Individuals, Same Bank):** The user loads statements of multiple people from one bank branch or group. Cross-statement analysis finds transactions linking these individuals (e.g. many payments among them) and flags collective anomalies. This can uncover syndicates or coordinated layering.

- **Statements (Different Individuals, Different Banks):** The user ingests batches from various accounts at different banks. The system's cross-link engine correlates by common payees, addresses, phone numbers, etc., and builds network graphs spanning banks. This supports multi-jurisdictional investigations and exposes hidden relationships.

In all workflows, the module applies its full analytics suite. For example, it links accounts if multiple statements share common counterparties or addresses, enabling visualization of complex networks. It also runs AML rules on the combined data set, so that fraud or AML alerts fire on transactions spanning multiple files. Prebuilt analytics (Summary, Overview, Transactions, Recurring Payments, Counterparties) update dynamically as statements are added. Importantly, each workflow supports cross-link analysis and fraud detection: users can navigate from a high-level summary into visual graphs or transaction details to investigate anomalies across any combination of statements.

3. Core Features

- **Rules-Based AML/Fraud Detection Engine:** The core engine applies configurable red-flag rules to all transactions. It comes with 15 preloaded rules based on Indian AML standards and common fraud patterns (see next section). Rules cover cash thresholds, round-trip transfers, unusual account activity, etc. The engine scores or flags accounts when rules trigger, and calculates an overall risk score. An admin UI ("configurator") allows users to enable/disable rules or define new ones (e.g. adjust amount thresholds). This aligns with RBI and FIU guidance: RBI mandates software that "throws alerts when transactions are inconsistent with risk categorization". Our module likewise auto-alerts on suspicious patterns, while still allowing customization to local policies.

- **Link Analysis Module:** The system provides an interactive graph view of transactions and entities. Each node is an account or counterparty; edges represent flows. The visual flow of funds helps identify *circular transactions* (funds routed back to origin), *round-robin transfers* (funds shuttled among multiple accounts), and unusually large movements. For example, network analysis can "easily identify suspicious patterns" like circular transaction cycles and smurfing (breaking large transfers into many small ones). The graph view is scalable and interactive: users can zoom, filter by counterparty, or highlight specific flows (e.g. cash withdrawals). Link analysis simplifies spotting collusive behavior that tabular views miss. The module also supports exporting these visual graphs: users can save the network diagram as an image (PNG/JPG) or embed it in reports (PDF) for inclusion in case files.

- **PDF Authenticity Verification:** Each uploaded PDF is automatically checked for tampering or forgery. The module compares document metadata and fonts against known bank statement templates. It flags manipulated files (e.g. altered statements) with an “Authenticity Status” (Original/Review/Fraud/Unknown). This prevents fraudsters from subverting the analysis by submitting fake documents. (For example, vendors like DocuClipper note that AI can “detect fraudulent documents, tampering attempts” in statements.) If a PDF fails authenticity checks, the user is alerted to inspect or reject it.

- **Analytical Report Sections:** Once analysis runs, the UI provides several tabs and report sections. Key views include:
  - **Summary:** High-level metrics (account balance ranges, totals, overall risk score) and counts of rule hits or suspicious transactions.
  - **Overview:** Visual trends (balances over time, cash flow charts) and metrics per period.
  - **Transactions:** A ledger view of all extracted transactions, filterable by type, amount, or date. Suspicious items are highlighted (e.g. large cash credits).
  - **Recurring Payments:** Identifies any repeated payments (inflows or outflows) by merchant or amount, flagging unusual subscriptions or potential money mules.
  - **Monthly Counterparties:** Shows the number of unique counterparties per month, helping detect bursts of new contacts.
  - **Counterparty Analysis:** Lists counterparties with totals and risk info (e.g. PEP status); highlights common payees across accounts.For instance, the reports should emphasize patterns (“minutest details such as red flags, spending patterns, obligations”) across multiple accounts and banks. Our module breaks down data into actionable reports, supporting both overview and deep-dive workflows.

4. Detailed AML/Fraud Detection Rules

The system ships with 15 predefined rules, each triggered by specific transaction patterns. Rules are based on regulatory guidelines and common fraud cases in India. Each rule below includes rationale and compliance context:

1. **Large Cash Deposits:** Flag cash credits exceeding a threshold (e.g. ₹10–50 lakhs) or an unusually large deposit given the account’s history. Rationale: Big unaccounted cash is a classic money-laundering red flag. RBI’s list of suspicious activities highlights large cash transactions as suspect, especially if inconsistent with business. Compliance: Cash above ₹10,00,000 typically requires a CTR to FIU-IND, so unreported cash near or above this limit is risky. Income Tax rules (Sec. 269ST) also

forbid cash receipts above ₹2 lakh, making such deposits illegal.

2. **Large Cash Withdrawals:** Flag unusually large withdrawals or sequences of withdrawals. Rationale: Quickly pulling out cash can indicate layering or funding of illicit activities. For example, excessive cash ATM withdrawals have been noted in money-laundering schemes. Compliance: Large cash withdrawals may bypass CTR reporting thresholds if split; RBI AML rules warn of “integrally connected cash transactions” to catch structuring.

3. **Structuring/Smurfing:** Multiple transactions just below reporting thresholds (e.g. many just under ₹10 lakh). Rationale: Customers splitting transfers to evade CTR/STR reporting is a known evasion tactic. RBI guidelines explicitly cite “several cash transactions below a specified threshold…to avoid the threshold limit”. The engine should flag a pattern of many near-threshold transactions as suspicious.

4. **Rapid In-and-Out (Circular Transactions):** Funds deposited then withdrawn immediately. Rationale: If deposits are quickly withdrawn with no clear business need, it often means pass-through laundering. RBI’s list includes “transactions in which assets are withdrawn immediately after being deposited” as suspicious. Napier’s network analysis notes circular money movements (funds cycling back to origin) as a core ML pattern.

5. **Round-Robin Funds:** Money cycling among several accounts or entities in a loop. Rationale: Criminals move funds in round-robin to disguise origin. Napier identifies “circular transactions: funds moving in a cycle back to the original sender”. The module detects funds traversing a closed loop (A→B→C→A) beyond normal transactions.

6. **Mismatch with Business/Nature:** Large credits or debits inconsistent with declared business activity. Rationale: RBI cites “accounts with large volume of credits whereas the nature of business does not justify such credits” as suspicious. For instance, a small retail shop account suddenly receiving tens of lakhs from abroad. This rule compares transaction totals to known business turnover or past averages and flags anomalies.

7. **Unexplained New Counterparties:** A surge of transactions with new or random counterparties. Rationale: Many “one-time” payees (especially across borders) may indicate structured layering. The “Monthly Counterparties” report would spike. Compliance: If large payments are made to unknown or unrelated entities, it may violate KYC norms and trigger STR filing obligations under PMLA.

8. **Multiple Accounts Linked:** The same customer name, PAN, address, or phone number on multiple accounts. Rationale: Criminals often open straw or proxy accounts (“benami” accounts) to hide activities. RBI lists “multiple accounts under the same name” as a signal. The Hindustan Times **2025** case of 25 proxy salary accounts is a real example. The rule flags when one person appears on many accounts, especially with overlapping transactions.

9. **Frequent Overdrafts/Credit:** Repeated use of OD or cash credit facilities. Rationale: Taking multiple overdrafts or heavily relying on bank credit may indicate cash flow manipulation. Excessive OD usage with no clear need can hint at circular financing. (Finezza highlights “too many overdrafts” as a red flag for strained or suspicious finances.)

10. **Multiple Bounce-Cheques or Payment Failures:** Numerous returned cheques or late EMI/bill payments. Rationale: Failed payments often occur when funds are being siphoned or accounts are empty due to fraud. Finezza notes “too many bounced cheques, due to lack of cash” as a warning sign. Repeated transaction failures are flagged.

11. **High-Volume Wire Transfers:** Repeated large outbound remittances or inward transfers, especially with high-risk jurisdictions. Rationale: Strange high-value wires can indicate funds moving out of the country illicitly. RBI’s AML norms require screening transfers to/from sanctioned or high-risk locations. The module flags repeated wire transfers over a threshold, especially if counterparties are foreign.

12. **PEP or High-Risk Counterparty:** Transactions involving Politically Exposed Persons or sanctioned entities. Rationale: PMLA and RBI guidelines demand enhanced scrutiny of PEPs. If a payee or payer is on sanctions lists or PEP lists (automatically checked), the rule triggers.

13. **Inconsistent Income/Expense vs. Declared Salary:** Large net inflows beyond declared income (e.g. a salary account suddenly shows multiple lacs of deposits). Rationale: Indicates unreported income or laundering. Indian KYC norms and Income Tax filings require consistency between declared financial standing and transactions. Discrepancies may imply tax evasion or hidden sources (violating Income Tax Act provisions on unaccounted income).

14. **Repeated Small Inflows (Layering):** Many small deposits from multiple sources followed by a large lump sum outflow. Rationale: This is classic layering – breaking illicit funds into small parts to slip under radars. The system detects when numerous small credits (e.g. from various accounts) feed a large outflow.

15. **High Cash Score or Volatility:** Accounts with extreme balance swings or volatility. Rationale: A volatility score (like Precisa’s volatility metric) flags erratic cash flows. An account that alternates between near-zero and very high balances is suspect. The rule raises an alert when the standard deviation of daily balance is unusually large relative to turnover, in line with RBI’s “sudden surge in activity” note.

Each rule is designed to map to regulatory concerns. For example, Rule 3 addresses RBI’s warning against splitting transactions; Rule 8 enforces RBI’s “no multiple fictitious accounts” principle; Rule 15 aligns with RBI’s “sudden surge in activity” catchall. Users can adjust thresholds or disable rules as needed. All triggered rules log evidence (transaction details, matched criteria) so analysts have audit trails when filing STRs under PMLA.

5. User Stories

1. *As a fraud investigator*, I want to upload a suspect's bank statement PDF and quickly see if any transactions violate known AML rules, so that I can prioritize the case. (E.g. I upload one statement and get immediate highlights: large cash deposits, multiple transfers to shell companies, etc.)

2. *As a fraud investigator*, I want to load multiple accounts from one individual's different banks and see a consolidated analysis, so I can detect cross-bank money laundering schemes. (Uploading statements from Bank A and Bank B for the same customer shows linkages and an overall risk score.)

3. *As a law enforcement analyst*, I want to load statements of several people and have the system draw a network graph of all inter-personal transactions, so that I can uncover a money mule ring. (Uploading three suspects' statements reveals circular fund flows between them, as shown in the link analysis graph.)

4. *As a law enforcement analyst*, I want to verify the authenticity of a customer's submitted statement file, so that I can avoid being deceived by forged documents. (After the customer uploads a PDF, the module labels it "Original" or "Fraud," prompting manual review if needed.)

5. *As a law enforcement analyst*, I want the module to export all generated charts and tables (especially the link analysis graph) to PDF or image, so I can include them in an external case report system. (After analysis, I hit "Export" and get a ZIP of graphs and CSV data ready to attach to our investigations database.)

These stories demonstrate practical usage: single- and multi-statement analysis, network detection, PDF verification, and integration/export.

6. Data Sources and Input Formats

The module supports input in common statement formats:

- **PDF**: Both native (text PDF) and scanned images. The system uses OCR and layout parsing to extract fields (dates, amounts, payees) from diverse bank templates. As noted by Precisa, a good analyzer "converts PDF files…to formats that are easy to read, such as CSV and Excel". Our tool similarly transforms unstructured PDF data into a structured database of transactions.

- **Excel/CSV**: For banks or customers providing statements in spreadsheets, the system ingests these directly (matching columns by heuristics).

- **Transaction Records**: It may also accept raw transaction exports (MT940/MT942, JSON, etc.) if available.
  The emphasis is on accurate **unstructured-to-structured conversion**: complex

PDF pages (multi-column, rotated text, handwritten notes) are parsed so that every transaction line is captured in our database. Once structured, all analytics (rules, flows, visualizations) operate on the unified dataset. The ETL process preserves metadata (account number, IFSC, statement date range) for record-keeping.

7. Compliance References

This module is built to align with key Indian AML regulations:

- **Income Tax Act, 1961:** Transactions are screened for violations of tax provisions (e.g. Sec. 269SS/269T ban on cash loans/deposits above ₹20,000) and unreported income. The rules engine includes checks for suspicious income/expense levels relative to declared income. Any detected pattern of tax evasion (e.g. undisclosed interest income, bogus expenses) can be highlighted for investigators.

- **PMLA 2002:** All suspicious findings support the PMLA framework. The system logs flagged transactions so that an FIU-IND STR can be filed “within 7 days” of concluding suspicion. Compliance requires maintaining records for 10 years; our module retains all parsed data and report snapshots accordingly. Alerts are conservative to ensure timely STRs. (As per RBI, a robust alert system is “essential for effective identification and reporting of suspicious transactions”.) The software’s audit trails directly feed into STR documentation.

- **RBI KYC/AML Guidelines:** RBI’s master circulars list many of our red flags. For instance, RBI’s Annex-V highlights “transactions involving large amounts of cash” and “moving the same funds repeatedly among several accounts” as suspicious; our rules cover these cases. RBI also requires periodic review of risk profiles and ongoing monitoring; this module operationalizes that by recalculating risk scores on new statements and notifying if customer risk changes. We also incorporate RBI’s sanctions- and PEP-check requirements: accounts or transactions linked to banned entities are flagged. In short, the module’s rules and alerts map to guidelines under PMLA and RBI (e.g. covering the “indicative list of suspicious activities” in RBI’s KYC norms).

8. Export and Integration

- **Analytics Export:** Users can export any chart or graph as PNG/JPEG. In particular, link-analysis graphs (network diagrams) can be saved or printed for reports. Tables and lists (transactions, counterparties) can be exported to Excel or CSV for offline review. Full reports (summary, metrics) can be compiled into PDF reports. For example, after reviewing the link graph, a user might click “Download PDF” to embed the chart into a case folder.

- **API Integration:** The module exposes RESTful APIs for seamless integration. External systems (e.g. case management or fraud platforms) can push statements via API and retrieve analysis results. Alerts and evidence can be fetched programmatically. Conversely, when our module flags an issue, it can push an alert or report to a third-party case system (e.g. law enforcement databases or bank's AML case management) via webhook or API. This ensures that analysis feeds directly into investigators' workflow. (Comparable AML solutions note case-management integration: e.g. Seon's AML SDK integrates alerts into a case system.)

9. UI/UX Notes

The user interface follows the style indicated by provided screenshots: a clean dashboard with tabbed sections for Summary, Overview, Transactions, etc. Key metrics (average balance, max/min, risk score) appear in header cards. The design uses data visualizations (charts, graphs) consistent with the sample UI. For example, the Summary/Overview screens should highlight alert counts and balance charts as shown in the reference screenshots. The color-coding and layout (tabs on top, data grids, export buttons) will mirror those examples. Transaction lists can be filtered/sorted, and irregularities are shown in a dedicated tab (as in Irregularities [3780] in the screenshot). Overall, the UX is report-centric and intuitive for forensic analysis – users click into flags to drill down on details.

10. Security and Access Control

- **Secure Access:** All data transmissions use TLS encryption. Uploaded files and analysis results are stored encrypted at rest. As stated by industry examples, the system employs "enterprise-grade encryption" for documents.

- **Authentication & Permissions:** Role-based access control ensures only authorized users can view sensitive data. Typical roles include Analyst (can view and flag data), Investigator (full view, export rights), and Admin (rule configuration, user management). Each user must log in via SSO or strong credentials.

- **Audit Logs:** Every user action (file upload, analysis run, rule edit) is logged with timestamp and user ID. The system maintains an audit trail of who accessed which statements and what findings were reported. This audit log supports regulatory compliance and internal audits.

- **Data Isolation:** For multi-tenant environments (e.g. separate law enforcement agencies vs. banks), data is logically partitioned. Users see only the accounts they are authorized for. All data exports carry a security watermark to discourage unauthorized sharing.

- **STR Filing Confidentiality:** Following RBI rules, once a suspicious alert is generated, the module locks the record against customer notification (no tipping-off) and notes it for STR filing. The principal officer role (or equivalent) can review alerts and finalize them; the system assists by requiring justification text for each STR.

In summary, the module not only automates AML analytics, but does so in a secure, compliant manner. It aligns with Indian AML/KYC laws (Income Tax Act, PMLA, RBI guidelines) and provides law enforcement/BFSI users with the tools and workflow to investigate financial crime efficiently. All features, from rule customization to link-graph export, are designed to support real cases and regulatory requirements.