REMI: AI-Driven AML and Fraud Detection: Automating Forensic Accounting for Faster, Smarter Investigations

Uncover complex financial crimes, money laundering, and fraud in minutes with AI-powered automation and advanced forensic analysis.

The 50 forensic accounting detections in REMI are a comprehensive set of AI-driven rules and pattern-recognition algorithms designed to flag suspicious financial activities, from unauthorized transactions to complex money laundering schemes. These detections analyze transaction patterns, vendor relationships, account structures, and unusual financial behaviors to uncover hidden fraud, tax evasion, asset misappropriation, and other financial crimes. By automating the detection process, REMI enables forensic accountants to quickly identify and investigate red flags, trace funds, and link activities across accounts, entities, and locations, significantly reducing the time needed for thorough financial crime analysis and allowing them to focus on building a clear, actionable case.

Forensic Accountant Detection Rules

1. **Unauthorized Access to Sensitive Financial Data**
   Detects unauthorized attempts to access or modify sensitive financial data files or records.

2. **Unusual Account Structure or Layering**
   Flags accounts set up with complex structures or excessive layering, a common tactic in money laundering.

3. **Frequent High-Risk Jurisdiction Transfers**
   Identifies frequent transfers to or from high-risk countries or offshore tax havens.

4. **Sudden Changes in Transaction Patterns**
   Detects sudden shifts in transaction volume, frequency, or type, which may indicate fraudulent activity.

5. **Round-Number Transactions**
   Flags transactions that frequently involve rounded amounts, which may mask illicit financial transfers.

6. **Rapid Fund Movement Across Accounts**
   Detects funds moving rapidly between accounts in a short period, possibly indicating layering or structuring.

7. **Duplicate Vendor Payments**
   Identifies instances where vendors are paid multiple times for the same invoice or service.

8. **Unapproved Journal Entries**
   Flags journal entries that bypass normal approval workflows, particularly for high-value transactions.

9. **Unusual Asset Revaluation**
   Detects significant changes in asset valuations that deviate from expected accounting standards.

10. **Frequent Changes in Vendor Bank Details**
    Flags changes in vendor payment information, which may signal vendor fraud.

11. **Payments to Unlisted Vendors**
    Identifies payments made to vendors not listed on the approved vendor list.

12. **High-Volume Small Transactions**
    Detects high volumes of small transactions that collectively reach significant amounts, often used to evade detection thresholds.

13. **Late-Stage Adjustments to Financial Statements**
    Flags financial statement adjustments made near reporting deadlines.

14. **Unusual Depreciation Methods**
    Detects non-standard depreciation rates or methods applied to specific assets, which could indicate manipulation.

15. **Excessive Write-Offs in Specific Accounts**
    Flags accounts with abnormally high write-offs that may be used to conceal fraudulent transactions.

16. **Unusual Payroll Activity**
    Identifies irregular payroll transactions, such as payments to inactive or terminated employees.

17. **Employee Expense Anomalies**
    Detects employee expense claims that deviate from established policies, such as excessive meal or travel expenses.

18. **Round-Tripping Transactions**
    Identifies transactions where funds appear to be moved in a circle between entities, inflating revenue or masking real ownership.

19. **Inflated Invoices or Payments to Shell Entities**
    Flags high-value invoices or payments to entities with minimal or no operational presence.

20. **Suspicious Charitable Contributions**
    Detects large or unusual charitable donations, potentially used for tax evasion or as a means to funnel funds.

21. **Asset Misappropriation Through Personal Expenses**
    Identifies instances where personal expenses are misclassified as business expenses.

22. **Structured Deposits to Avoid AML Reporting Thresholds**
    Flags deposits that are structured just below AML reporting thresholds, often to avoid scrutiny.

23. **Rapid Employee Turnover in Financial Roles**
    Detects unusual patterns in employee turnover within finance-related positions, potentially to facilitate fraud.

24. **Ghost Vendors**
    Identifies vendors with incomplete or suspiciously similar information to existing entities.

25. **Vendor Kickback Schemes**
    Detects patterns indicating kickbacks, such as inflated vendor invoices or payments to vendors linked to employees.

26. **Related-Party Transactions**
    Flags transactions between related parties or employees and vendors, indicating potential conflicts of interest.

27. **Abnormal Loan Issuances or Forgiveness**
    Detects loan issuances or forgiveness that deviate from standard company practices.

28. **Sequentially Numbered Invoices from Vendors**
    Flags vendors submitting consecutively numbered invoices, potentially to conceal fraudulent billing.

29. **Significant Changes to Revenue Recognition**
    Detects adjustments to revenue recognition practices, often used to manipulate reported earnings.

30. **Frequent Tax Filing Adjustments**
    Identifies recurring adjustments in tax filings, indicating potential tax evasion tactics.

31. **Duplicate or Phantom Employees in Payroll**
    Detects employees on payroll who do not have corresponding HR records or active roles.

32. **Misclassification of Liabilities and Expenses**
    Flags instances where liabilities or expenses are misclassified to manipulate financial results.

33. **Unusual Refund or Rebate Activity**
    Detects refunds or rebates issued at abnormal frequencies or amounts, often to benefit associated parties.

34. **Sudden Cash Withdrawals Above Normal Levels**
    Flags large cash withdrawals that deviate from typical patterns, potentially indicating fraud.

35. Frequent Inter-Company Transactions Without Justification
Detects high volumes of inter-company transactions that lack a clear business purpose.

36. Off-Balance Sheet Transactions
Identifies unrecorded transactions that should be reflected on the balance sheet.

37. Patterns Indicating Ponzi or Pyramid Schemes
Flags suspicious patterns where funds from new clients are used to pay returns to earlier clients.

38. Unauthorized Changes to Payment Terms
Detects changes to vendor payment terms without documented approvals.

39. Frequent Use of Petty Cash for Large Purchases
Flags high-value purchases made using petty cash, which may indicate an attempt to bypass accounting controls.

40. Unusual Growth in Accounts Receivable
Identifies rapid increases in accounts receivable balances, potentially to inflate reported revenue.

41. Multiple Transactions with Same Beneficiary
Flags cases where multiple entities make payments to the same external account, suggesting possible kickbacks.

42. Shell Company Transactions Involving Layered Transfers
Detects transactions that move through multiple layers or entities, often a tactic for money laundering.

43. Non-Standard Lease or Rental Agreements
Flags lease or rental payments that deviate from market rates, potentially hiding asset misappropriation.

44. Significant Adjustments in Accounts Payable
Detects large or frequent adjustments to accounts payable, possibly indicating manipulation of liabilities.

45. Unusual Investment in Non-Core Business Activities
Flags investments in businesses unrelated to the core company, a possible vehicle for asset diversion.

46. Inconsistent Forex Transaction Patterns
Identifies foreign exchange transactions that deviate from typical trading patterns, possibly concealing currency manipulation.

47. High Ratio of Cash to Credit Sales
Flags businesses with disproportionate cash sales relative to credit, a possible indicator of tax evasion.

48. Frequent Adjustments to Fixed Assets
Detects recurring adjustments to fixed assets that could be attempts to manipulate depreciation or asset value.

49. **Large Gifts or Loans to Executives**
Flags high-value gifts, loans, or advances made to executives that lack a clear business purpose.

50. **Related Entity Cash Transfers Without Documented Purpose**
Identifies cash transfers between related entities without documented explanations, indicating potential misappropriation.