REMI: Financial Crimes Categories

Revolutionize Financial Crime Detection with AI-Driven Insights

REMI offers financial crime investigators a powerful, interactive experience with adjustable controls for every detection. Each detection rule includes customizable settings, allowing investigators to fine-tune sensitivity, thresholds, and behavior analysis parameters directly within the platform. This tailored approach ensures REMI adapts seamlessly to specific investigative needs, enabling a precise and efficient detection pipeline. With REMI, investigators can quickly adjust and refine detections, optimizing results in real time.

Unauthorized Access Patterns

Detects access to sensitive financial data by unauthorized users, especially those who exhibit unusual access patterns outside normal working hours.

Vendor Payment Changes Without Authorization

Flags changes in vendor payment details that lack proper authorization, which could indicate potential vendor fraud or account manipulation.

Tax Inconsistencies

Compares reported tax amounts against calculated values, identifying discrepancies that may indicate misreporting.

Duplicate Invoice Payments

Detects instances where identical invoices are paid more than once, either accidentally or as part of a fraudulent scheme.

Unapproved Journal Entries
Flags journal entries that bypass normal approval workflows, particularly those involving high-value transactions.

Suspicious Internal Transfers
Identifies internal fund transfers that deviate from typical patterns or involve unexplained large amounts.

Missing Audit Trails
Flags missing or incomplete audit trails, indicating potential attempts to erase transaction history.

Credit Card Misuse
Detects unauthorized or personal use of corporate credit cards, especially for high-risk expense categories.

Sudden Payroll Increases
Flags unexpected payroll increases, especially for high-level positions, which may indicate misuse of funds.

Unapproved Expense Claims
Identifies expense claims that exceed thresholds or lack necessary receipts and approval.

Frequent Financial Reconciliations
Detects unusually frequent reconciliations in specific accounts, a tactic sometimes used to conceal irregularities.

Abnormal Depreciation Rates
Flags assets with depreciation rates that significantly deviate from industry norms.

Quarter-End Invoice Spike
Identifies a spike in invoice issuance or payment processing around quarter-end, indicating possible manipulation to meet financial targets.

Unapproved Vendors
Detects payments made to vendors who are not in the approved vendor list, a possible indicator of vendor fraud.

Frequent Vendor Contract Changes
Flags frequent modifications to vendor contracts, which could indicate unauthorized changes or manipulation.

High Write-Off Volume in One Department
Detects departments with unusually high volumes of write-offs, potentially masking improper transactions.

Large Cash Transactions Without Approval
Identifies cash transactions exceeding specified thresholds that lack supporting documentation.

Unusual Credit Card Reimbursements
Flags credit card reimbursements that deviate significantly from typical spending patterns for the role or department.

Forecast Manipulation
Identifies irregularities in forecast adjustments that are not linked to documented business changes.

Duplicate or Inflated Invoices
Detects duplicate or unusually high-value invoices that deviate from standard pricing.

Unusual Travel Expenses
Flags travel expense claims that exceed standard rates or are not linked to documented business purposes.

Abnormal Inter-Company Transactions
Identifies inter-company transactions that do not follow expected patterns, potentially masking fund transfers.

Unexplained General Ledger Adjustments
Flags general ledger adjustments that lack detailed explanations or supporting documentation.

Ghost Vendors
Detects vendors with minimal or suspiciously similar business information, potentially set up to funnel funds.

End-of-Year Transaction Surge
Identifies a high volume of transactions around the fiscal year-end, possibly inflating financial results.

Abnormal Asset Valuation Changes
Flags unusual changes in asset valuations that could be tied to manipulation of financial statements.

Multiple Bank Accounts for Single Employee
Detects employees with multiple linked bank accounts, potentially diverting payroll funds.

Small Transactions Pattern
Identifies a pattern of small transactions that collectively exceed approval limits, a tactic used to evade detection.

Expense Spike in Specific Categories
Flags specific expense categories with sudden increases, potentially indicating misuse.

Round-Number Transactions
Detects transactions with rounded amounts, which may be used to simplify fraudulent reporting.

Transaction Splitting
Flags transactions that appear to be split to avoid approval thresholds, indicating potential fund misuse.

Duplicate Employee Profiles
Identifies duplicate employee records, which could indicate payroll fraud.

Sudden Drop in Receivable Turnover
Flags a significant drop in receivable turnover ratio, indicating potential revenue manipulation.

Same-Day Approval for High-Value Transactions
Detects high-value transactions that receive same-day approval, potentially bypassing due diligence.

Payment Date Adjustments Without Justification
Flags payment date changes that lack formal approval, possibly to delay reporting obligations.

Round-Tripping
Detects round-tripping, where funds are moved back and forth between entities to inflate transaction volumes.

High Initial Payments to New Vendors
Identifies new vendors receiving large initial payments, which may indicate kickback schemes.

Unusual Weekend or Holiday Expenses
Flags expenses submitted for weekends or holidays that lack exceptional justification.

Frequent Foreign Transactions
Identifies frequent foreign transactions that deviate from usual business activity.

Sequentially Numbered Invoices
Detects suspiciously sequential invoices, which may indicate fictitious vendor arrangements.

No-Receipt Reimbursements
Flags reimbursements above thresholds submitted without receipts, potentially indicating misuse.

Suspicious Charity Contributions
Detects large or unusual contributions to charities, which may be used as a vehicle for fund diversion.

Similar Vendor Names
Identifies vendors with nearly identical names, potentially set up to avoid detection while transferring funds.

Inventory Write-Off Anomalies
Flags inventory write-offs that deviate from usual patterns, potentially covering asset misappropriation.

Frequent Payment to Related Entities
Detects payments to entities with ties to employees or executives, a red flag for self-dealing.

Abnormal Reserves Adjustments
Identifies significant adjustments in reserve accounts, possibly to manipulate reported income.

Unusual Expense Growth Rates
Flags categories with rapid expense growth that lacks corresponding business expansion.

Personal Accounts Used in Transactions
Detects instances where funds are directed to personal accounts linked to employees.

Excessive Write-Off of Receivables
Flags high write-offs in receivables, potentially indicating revenue manipulation or asset diversion.

Vendor Profile Changes Without Documentation
Detects frequent changes to vendor profiles that are not supported by corresponding documentation.