



FIRE Technical Overview

Financial Intelligence & Reconciliation Engine • For Forensic Accountants and Litigation Attorneys

FIRE is a purpose-built forensic financial investigation platform that automates the complete workflow from raw data ingestion through court-ready report output. It is designed specifically for the standards of forensic practice, not adapted from general-purpose accounting software. Every output artifact carries a cryptographic chain of custody, every finding is traceable to its source record, and every report is structured for evidentiary use.

Platform Specifications

Current version	V5.0.0 (40+ discrete development iterations)
Operating modes	Forensic Investigation Proof of Cash Reconciliation Asset Tracing (bank-statement-only)
Data inputs	Bank statements and general ledger files (.xlsx, .csv), with auto header detection across rows 1 to 12
Matching engine	Four-pass: exact amount, fuzzy date tolerance, payee normalization, partial match
Fraud detection	Ten-signal composite scoring engine with configurable rule weights
Risk classification	Five-tier: Critical, High, Moderate, Low, Clean
Chain of custody	SHA-256 cryptographic hash of source files at ingestion, embedded in all output
Multi-account support	Multiple concurrent bank accounts; cross-account transfer reconciliation and tracing
Output formats	Court-ready PDF report plus a structured Excel workbook
Source traceability	Persistent sequential source reference ID on every transaction, from ingestion through report
Deployment	Windows desktop application; runs entirely offline, data never leaves the examiner's computer
Patent status	Utility patent application filed; Track One prioritized examination granted (accelerated review). Patent pending.

Forensic Investigation Mode

The forensic investigation engine applies a multi-pass reconciliation algorithm followed by a composite fraud scoring pass across 100% of ingested transactions. The process is fully automated and produces findings ranked by risk tier with complete source documentation.

Reconciliation Engine

- **Pass 1, Exact Match:** Amount, date, and payee match within a defined tolerance. Highest-confidence matches resolved first.
- **Pass 2, Fuzzy Date Match:** A configurable date window (plus or minus 3 days by default) accommodates float, cutoff differences, and posting delays.
- **Pass 3, Payee Normalization:** Vendor name standardization resolves abbreviations, punctuation, and DBA names before matching.
- **Pass 4, Partial Match:** Remaining unmatched items are evaluated for split payments, partial postings, and timing differences.

Ten-Signal Composite Fraud Scoring

Each transaction is scored across ten concurrent signals. Signal weights are configurable; composite scores determine risk-tier assignment.

Capability	Technical Description	Professional Application
Round Dollar Amount	Flags transactions with no cents component above a configurable threshold	Structured payments, fictitious vendor schemes, petty cash manipulation
Just-Below Threshold	Detects disbursements just under approval thresholds	Authorization bypass, a primary indicator in procurement fraud
Duplicate Payment	Same-payee, same-amount transactions within a rolling 30-day window	Double-billing, accidental duplicates, fictitious invoices
Cash Withdrawal	Flags ATM and cash disbursements by type and amount	Unsubstantiated cash expense, skimming, personal use of entity funds
Rapid Repeat	Same-payee transactions in rapid succession	Vendor collusion, split-invoice schemes, fictitious repeat billing
Weekend / Holiday	High-value transactions posted on non-business days	Reduced-oversight periods common in unauthorized disbursements
New Vendor	Payees with no prior transaction history in the dataset	Ghost-vendor schemes; new vendors with immediate large payments
Vendor Outlier	Payees whose amounts deviate from their own baseline	Billing inflation by established vendors
Year-End Journal Entry	Five-signal composite on late, round, unusual, override, unsupported entries	Revenue manipulation, liability concealment, bonus fraud
ACH Differentiation	Three-pass classification of internal vs external transfers	Eliminates false positives on treasury transfers; isolates suspicious ACH

Proof of Cash Mode

The Proof of Cash engine constructs a complete four-column reconciliation schedule for any defined period, cross-referencing bank activity against general ledger postings with forensic-grade exception documentation. It supports multiple bank accounts, reconciling each account to its own ledger account and then combining them, with transfers between the accounts detected and netted.

Schedule structure	Beginning Balance Receipts Disbursements Ending Balance
Reconciling items	Outstanding checks, deposits in transit, and unposted items identified and classified
Exception tagging	Each unreconciled item assigned a fraud risk classification from the scoring engine
Period support	Any calendar or fiscal period; multi-period sequential analysis supported
Statement tie-out	Computed balances tied back to the balances the statements themselves report
Legal exhibit use	Formatted as a standalone exhibit; the chain-of-custody hash ties the report to source files

Asset Tracing Mode (New in Version 5.0)

Asset Tracing analyzes bank statements on their own, with no general ledger, for divorce, estate, and fraud engagements where the books are unavailable or in dispute. It inventories every account, ties each statement out month by month, traces money moved between the client's own accounts, and separates true external cash flow from internal transfers so the totals are not inflated. It is deterministic and never guesses: a movement that could be explained more than one way is shown but not netted.

Capability	Technical Description	Professional Application
Account Inventory & Tie-Out	Opening, deposits, withdrawals, and computed closing for every account, tied to the statement's own ending balance, month by month	Establishes the complete account population and confirms each statement is internally consistent
Transfer Inference	Cross-account matching of one-to-one, composite many-to-one and one-to-many, and multi-hop chains, netted only when the statement describes a transfer	Traces money moved between accounts, including a deposit split across several accounts on the same day
External vs Internal	Matched internal transfers are separated from third-party money so external totals are not inflated by funds shuffled between accounts	True money in and out of the marital or business estate
Unknown-Source Deposits	Each deposit reconciled to an internal transfer, interest, or an identified payer; the remainder is flagged and totaled by account and year	Undisclosed income; deposits with no known source
Counterparty Checklist	Every account money moved with; any account referenced but not provided is flagged to obtain	Undisclosed or hidden accounts; the account you were never given
Court-Ready PDF	A FIRE-branded exhibit with owner tagging and a balance timeline, generated with the workbook	A hand-ready exhibit for counsel, sourced and reproducible

Chain of Custody & Evidentiary Standards

- **SHA-256 Source File Hashing:** Every source file is cryptographically hashed at ingestion. The hash is embedded in the PDF cover page and the Excel metadata, so any later alteration of the source produces a different hash.
- **Source Reference Traceability:** A persistent sequential identifier is assigned to every transaction at ingestion and carried unchanged through matching, scoring, and reporting. Every flagged item references its exact source row.
- **Run ID Binding:** A unique Run ID ties the PDF, the Excel workbook, and the audit log to a single analysis session; re-running preserves prior runs as separate artifacts.
- **Audit Log:** A structured trail records session parameters, file hashes, rule configuration, and timestamps, included in the workbook and available for discovery.
- **Investigator Review Workflow:** A review queue presents flagged items in priority order with rule-hit documentation and disposition notes, producing a documented investigation record.

Evidentiary Note for Litigation Counsel

FIRE output is structured to support Federal Rules of Evidence 702 (expert testimony) and 803(6) (business records). The chain-of-custody hash authenticates the data analyzed, and the source reference system provides the traceable, repeatable methodology an expert needs to defend findings under cross-examination. FIRE does not alter source data; all analysis runs on normalized copies and originals remain verifiable against the embedded hash.

Professional Applications

Family Law and Marital Dissolution

- **Hidden-asset and account identification:** Asset Tracing names accounts money moved to or from that were never disclosed, and flags deposits with no identified source.
- **Dissipation of marital assets:** Rapid-repeat, just-below-threshold, and cash-withdrawal signals identify systematic diversion of funds around a dissolution.
- **Business income verification:** Proof of Cash on a closely-held entity confirms or contradicts reported distributions and compensation.

Forensic Accounting and Litigation

- **Fraud investigation:** Full-population analysis with composite scoring replaces sampling; coverage is 100% and documentation is automatic.
- **Expert-witness support:** Source reference IDs and chain-of-custody documentation provide the traceable methodology required for admissible opinion testimony.
- **Damage quantification:** The Proof of Cash schedule provides a defensible, independently verifiable accounting of cash flows for any period.

100%transaction coverage, no
sampling**SHA-256**chain of custody on every
output**3 modes**Forensic, Proof of Cash,
Asset Tracing**Patent
Pending**

novel forensic methodology