

FORENSIC ACCOUNTING & LEGAL PRACTICE GUIDE

Financial Statement Review Checklist

A standardized, step-by-step framework for forensic accountants, fraud examiners, and litigation attorneys conducting high-stakes bank and credit card statement analysis.

PHASE 1: INGESTION, COMPLETENESS & SOURCE VERIFICATION

1.1 File Integrity & Metadata Verification

Prerequisite

- ☐ **Verify Original File Hashes (SHA-256)**
Calculate and document baseline cryptographic hashes for all digital PDF, CSV, and OFX source files prior to parsing or extraction.
- ☐ **Statement Period Continuity Check**
Confirm contiguous date ranges across all accounts. Identify missing monthly statements or gaps in transaction history.
- ☐ **Opening & Closing Balance Reconciliation**
Cross-check reported starting/ending balances against calculated transaction sums to detect altered or missing ledger pages.

PHASE 2: PATTERN DETECTION & ANOMALY SCREENING

2.1 Financial Anomaly & Structuring Signals

Forensic Core

- ☐ **Near-Threshold Structuring Analysis**
Screen cash deposits and wire transfers occurring repeatedly between \$8,000–\$9,999 to identify potential CTR avoidance tactics.
- ☐ **Round-Dollar & Even-Sum Isolation**
Filter non-operating round-number payments (\$1,000, \$2,500, \$5,000) that often correlate with unrecorded loans or off-book transfers.
- ☐ **Peer-to-Peer & Cash App Aggregation**
Consolidate transactions involving Venmo, Zelle, Cash App, PayPal, and Wire transfers into a dedicated counterparty review ledger.
- ☐ **Lifestyle & Non-Business Expense Normalization**
Flag high-value luxury purchases, gambling, travel, and non-business vendors routed through corporate or shared accounts.

Data Confidentiality Notice (Local Processing Standard)

To maintain attorney-client privilege and work-product doctrine, ensure all forensic parsing, vendor normalization, and indexing occur 100% locally on an encrypted Windows workstation without uploading source statements to cloud services.

PHASE 3: DEEP INVESTIGATION & FOCUS AREA ANALYSIS

3.1 Hidden Asset & Unrecorded Account Discovery

Investigation

- ☐ **Inter-Account Transfer Matching**
Trace outgoing transfers and mortgage/credit payments to confirm both sides of every transaction match known, disclosed accounts.
- ☐ **Undisclosed Account Identification**
Flag outbound transfers to unfamiliar financial institutions, brokerage platforms, crypto exchanges, or foreign entities.
- ☐ **Recurring Subscription & Vendor Alias Normalization**
Map cryptic merchant descriptors and payment gateway codes (e.g., Square, Stripe) back to true legal entities and owners.

PHASE 4: COURT PREPARATION & EVIDENCE PACKAGING

4.1 Trial-Ready Work Product Assembly

Litigation Ready

- ☐ **Chronological Transaction Timeline Assembly**
Compile cross-account activity into a unified master timeline linked directly to original PDF page numbers and source exhibits.
- ☐ **Numbered Exhibit Generation & Indexing**
Assign standardized exhibit tags to source PDF statements and link each flagged transaction back to its exact source document page.
- ☐ **Manifest & Hash Chain Export**
Generate an exportable evidence manifest including source file paths, SHA-256 hashes, extraction logs, and audit trail metadata.
- ☐ **Workstation Security Archive**
Store complete case vault databases, reviewer notes, and encrypted backups on local, password-protected storage media.

Automate This Workflow with SharkAudit

SharkAudit for Windows automates every step in this checklist—from SHA-256 hashing and structuring detection to 1-click Court Prep exhibit packaging. All processing remains 100% local on your PC.

Explore editions and desktop licensing at sharkaudit.com