COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Digital Forensics in Corporate Fraud Investigations

Following the Money, the Documents and the Deception Through the Estate

Corporate fraud is a documents crime committed on computers: the false invoice raised in the ERP system, the doctored spreadsheet behind the covenant certificate, the side agreement that never reached the file, the payment redirected by a spoofed email, the two sets of books reconciled nowhere. Its investigation is therefore digital forensics with a financial spine: securing estates before suspects learn of suspicion, joining transactional records to the communications around them, exposing fabricated and backdated documents, tracing approval chains to real hands, and packaging findings for the multiple audiences fraud creates: boards, auditors, regulators, insurers, civil courts and sometimes the police. This guide gives UK lawyers and investigators the method: the fraud-pattern evidence map, covert-phase discipline, document-authenticity testing, the interviews-and-evidence sequence, and deployment across civil and criminal tracks without one poisoning the other.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Fraud work spans the laboratory's disciplines: covert-phase preservation, ERP and accounting-system extraction, document-authenticity examination, communications analysis and the choreography timelines that join them: reported under CPR Part 35 for civil claims and to criminal-evidence standards where matters are referred. The examples in this guide are fictional composites of the genre's standard patterns.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | FRAUD & FORGERY EXAMINATION | FINANCIAL-SYSTEMS FORENSICS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: fraud is documented by its own machinery

03 The fraud-pattern evidence map: schemes and their artefacts

04 The covert phase: preserving without alerting

05 Financial-systems forensics: ERP, accounting data and the communications join

06 Document authenticity: fabrication, backdating and alteration exposed

07 Deployment: civil, criminal, regulatory and the sequencing problem

08 Source architecture: where else the evidence lives

09 Worked examples

10 Common mistakes and technical limitations

11 Questions to ask · Suggested wording

12 Checklist and red flags · When to involve a digital forensic expert

13 Frequently asked questions

14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: FRAUD INVESTIGATIONS SUCCEED BY JOINING THREE RECORDS THE FRAUDSTER KEPT SEPARATE: THE MONEY'S TRAIL IN THE SYSTEMS, THE DOCUMENTS' TRUE HISTORY IN THEIR METADATA, AND THE COMMUNICATIONS AROUND BOTH: PRESERVED COVERTLY, JOINED FORENSICALLY, DEPLOYED IN THE RIGHT ORDER

The map (§3): each scheme type writes characteristic artefacts: invoice fraud lives in vendor-master changes, approval-chain records and payment-detail edits; payment-diversion lives in spoofed-domain emails and mandate-change trails; accounts manipulation lives in journal-entry patterns, spreadsheet lineage (guide 87's session evidence) and period-end timing; asset-stripping and side-deal fraud live in the unofficial channel (guides 63-66's messaging estates) beside the official file. **The covert phase (§4):** while suspects are unaware, the estate is preserved without footprints: server-side holds and log exports that touch nothing user-visible, imaging scheduled invisibly, scope decided by the §3 map: because the tip-off converts a rich estate into guide 95's gap problem overnight. **The joins (§5-§6):** financial-system extractions (guides 72-74's methods) are correlated with the communications and calendar record around each suspect transaction: who emailed whom the hour the journal posted: while questioned documents get guide 87 and 109's authenticity treatment: fabrication and backdating exposed from internal evidence. **Deployment (§7):** findings serve boards, auditors, insurers, regulators, civil claims (freezing and search orders on the forensic file) and criminal referral: sequenced deliberately, because privilege, self-reporting decisions and parallel-proceedings rules mean the order of disclosure is itself a strategic instrument.

- **Schemes have signatures:** the §3 map turns "we suspect fraud" into a targeted artefact list per scheme type.
- **Covert preservation first:** server-side, footprint-free, before interviews and before confrontation: §4's discipline.
- **The join convicts:** transactions, documents and communications correlated on guide 96's frame: the fraudster separated them; the investigation reunites them.
- **Authenticity is testable:** fabricated and backdated documents fail internal-evidence tests (§6): the forgery proved from its own file.
- **Sequence the audiences:** civil, criminal, regulatory and insurance tracks ordered with advice: §7's timing decisions are case decisions.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: fraud is documented by its own machinery

A fraud inside a company must use the company's machinery: payments go through the banking platform, invoices through the ERP system, approvals through workflows, documents through the DMS, and the coordination: because most frauds need coordination, or at least concealment from colleagues: through some channel, official or not. The machinery records. The fraudster's craft is keeping the records apart: the false invoice looks clean in isolation; the journal entry balances; the certificate reads plausibly: and hoping nobody joins the transaction to the vendor-master edit two days earlier, the approval routed around the usual chain, and the WhatsApp thread that says what the file does not.

The investigation's craft is the joining: which is why fraud forensics is this series' disciplines compounded: the financial extractions of guides 72-74, the platform logs of guides 51-58 and 105-107, the messaging estates of guides 63-66, the authenticity methods of guides 87 and 108-109, the gap analysis of guide 95, all normalised onto guide 96's timeline. And it is why the investigation's first risk is disclosure of itself: a suspect who learns the question is being asked can delete, coordinate stories and move assets faster than most organisations can preserve: §4's covert phase is not drama; it is the difference between the rich estate and the swept one.

§ 0 3 · THE MAP

The fraud-pattern evidence map: schemes and their artefacts

- **Invoice and procurement fraud:** vendor-master creation and edit logs (who added the supplier, when its bank details changed), approval-chain records and their bypasses, invoice-document lineage (guide 87: the "scanned" invoice generated by an office suite), duplicate-payment patterns, and the employee-vendor joins (shared addresses, phone numbers, beneficiaries) the structured data yields.
- **Payment diversion and mandate fraud:** the spoofed-domain and compromised-mailbox evidence (guide 80's fork: lookalike domains, header analysis), mandate-change requests and their verification trail (or its absence), rule and forwarding artefacts in the compromised account (guide 104), and the bank-side records of the redirected flow.
- **Accounts and reporting manipulation:** journal-entry forensics (round sums, period-end clusters, single-user patterns, reversals), spreadsheet lineage and session evidence behind certificates and covenants (guide 87's authoring artefacts), and the version ladder showing the numbers before they were improved (guide 75, guide 102).
- **Side deals and conflicts:** the unofficial channel beside the official file: personal email and messaging threads (guides 63-66), meeting and travel artefacts joining the parties, and the drafts that never entered the DMS: the deal's shadow record.
- **Asset and IP diversion:** guide 97's exfiltration map applied at management scale, plus corporate-structure and beneficiary evidence from registries and the OSINT layer (guide 129): where the value went, and to whom it traces.

§ 0 4 · THE QUIET FORTNIGHT

The covert phase: preserving without alerting

- **Need-to-know governance:** the investigation's existence restricted to a named circle (instructing lawyers, one or two executives, the examiners): with IT tasking framed as routine where IT staff sit outside the circle: because the leak that tips the suspect usually comes from helpfulness, not malice.
- **Server-side, footprint-free preservation:** litigation holds and log exports executed by admin mechanisms invisible to users (guides 51-58's machinery): mailboxes, drives and chat preserved without a flag the suspect can see; journaling and audit exports pulled centrally.
- **Invisible imaging:** device collection scheduled inside routine cover (refresh cycles, "security updates", overnight imaging with devices returned) where proportionate and lawful: with §5-of-guide-97's UK GDPR frame documented for the covert choices too.
- **The scope decided by the map:** §3's artefact list per suspected scheme drives what is preserved first: vendor-master logs and approval records for invoice fraud, mailbox and rule artefacts for diversion, journal and version stores for manipulation: breadth follows, but the signature evidence is secured in week one.
- **The confrontation gate:** interviews, suspensions and external notifications held until preservation is complete: the §4 phase ends by decision, not by accident: and the moment it ends, guide 97 §7's letters and orders stand ready for the personal estates the covert phase could not reach.

§ 0 5 · THE MONEY'S OWN RECORDS

Financial-systems forensics: ERP, accounting data and the communications join

- **Extract forensically, not by report:** ERP and accounting data pulled by the guide 72-74 disciplines: defined queries, documented scope, hash-verified exports: including the audit tables (who posted, edited, approved, when) that standard reports omit: the system's own story about its operators.
- **Pattern analytics with humility:** journal-entry testing (timing, amounts, users, reversals), duplicate and threshold analysis, vendor-employee matching: run as lead generation for the forensic join, with baselines respected: anomaly is a question, not a finding.
- **The communications join:** each suspect transaction correlated on guide 96's frame with the mail, messaging and calendar record around it: the journal posted at 17:42; the WhatsApp "done, post it tonight" at 17:31: the join that converts anomaly into narrative.
- **Approval-chain reconstruction:** workflow records tracing each authorisation to an account, then guide 105-107's attribution joining accounts to hands: delegation, credential-sharing and bypassed steps exposed as the control-failure evidence auditors and insurers need.
- **Quantification for every audience:** the transaction schedule (items, dates, amounts, counterparties, evidence references) built to serve simultaneously as the civil claim's schedule of loss foundation, the insurer's proof, and the referral bundle's core.

§ 0 6 · THE QUESTIONED DOCUMENTS

Document authenticity: fabrication, backdating and alteration exposed

- **Internal evidence first:** guide 87's method: creation and authoring artefacts against the claimed date (the 2019 agreement carrying a 2023 PDF library), font and resource availability, session and save-count evidence, and the guide 109 backdating signatures: the document convicted from its own file.
- **Lineage and the version ladder:** where the true history survives in DMS versions, drafts and email attachments (guides 75, 102), the fabricated item is bracketed: the "contemporaneous" minute absent from every contemporaneous store, the certificate's spreadsheet built in one session the week proceedings loomed (guide 82 Example 3's pattern).
- **The estate's negative testimony:** guide 95's existence analysis inverted: a genuine document of the claimed date should have left copies, references and transmission records: their systematic absence is itself evidence, stated with §10's honesty about limits.
- **Cross-copy comparison:** hash and content divergence across the "same" document's instances (guide 82 §7's copy-tracing): the counterparty's clean copy against the improved one in the file: the alteration localised to a custodian and a window.
- **Reporting to the standard the allegation needs:** authenticity findings drafted for CPR Part 35, with criminal-standard packaging where referral is contemplated: conclusions graded, alternatives addressed, the examiner's independence visible: forgery allegations are grave, and the report is built to carry them.

§ 0 7 · THE AUDIENCES

Deployment: civil, criminal, regulatory and the sequencing problem

- **The board and privilege:** the investigation structured for privilege from instruction (guide 91's dominant-purpose lessons, guide 97 §5's file): reporting lines, purpose records and the separation of legal advice from operational findings: decided on day one, because it cannot be retrofitted.
- **Civil remedies on the forensic file:** freezing injunctions and search orders where the evidence and risk support them: full-and-frank disclosure built on the examiner's affidavit: then the claim itself, with the §5 schedule and §6 reports as its spine, and guide 97's springboard-speed logic applying to dissipation risk.
- **Criminal referral weighed:** Action Fraud and force economic-crime units, the SFO where scale warrants: with advice on timing, because a live criminal investigation can stay civil proceedings and vice-versa considerations cut both ways: the referral is a strategic act, not a reflex.
- **Regulators, auditors and insurers:** FCA-regulated entities' notification duties, audit-relationship management (the auditors will ask for the file), and fidelity-insurance proof requirements: each audience served from the same evidence base, with disclosure to each weighed for privilege and prejudice.
- **Employment handled inside the strategy:** suspects' suspensions, interviews (with §4's gate respected) and dismissals run per guide 97 §5's process discipline: the unfair-dismissal flank guarded while the main tracks proceed.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: fraud evidence lives in the joins between estates, so the map is worked as a matrix: for every suspect transaction or document, the financial systems (ERP audit tables, banking records, journal stores), the platform layer (mailboxes, drives, chat, and their audit logs per guides 51-58, 105), the device layer (endpoints, phones, the messaging estates of guides 63-66), the counterparty record (the vendor's, bank's or buyer's copy of every exchange: the fraudster controls one side of a correspondence, never both), the external registries and OSINT layer (corporate filings, domains per guide 80, beneficial-ownership trails), and the paper-and-people layer (physical files, and witnesses whose recollections the digital record will test). When the primary source is compromised: books doctored, mailboxes purged, devices wiped: the matrix supplies the corrective: the bank's records against the doctored ledger, the counterparty's inbox against the purged one, the registry filing against the backdated agreement. Fraudsters can falsify what they control; the investigation wins on what they could not reach.

QUESTION	FINANCIAL SYSTEMS	PLATFORM LAYER	DEVICE / MESSAGING LAYER	COUNTERPARTY RECORDS	REGISTRIES / OSINT	DELETED/ RECOVERABLE
What moved, when	Y: postings + payments	Approval workflows	n/a	Y: bank + vendor side	n/a	Journal edit history
Who did it	Audit tables: accounts	Y: sign-ins + actions	Y: the hands layer	Their contact records	n/a	Varies
Was it coordinated	n/a	Mail + calendar joins	Y: the unofficial channel	Their half of threads	Shared infrastructure	Guide 95's routes
Is the document genuine	Posting-date brackets	Version ladders	Authoring artefacts	Y: the clean copy	Filing-date anchors	Prior versions often
Where did value go	Y: payment endpoints	n/a	Wallet + app artefacts	Receiving institutions	Y: ownership trails	Varies

Fallback strategy in one line: for every falsifiable record, hold its unreachable counterpart: bank against ledger, counterparty against custodian, registry against file: the fraud proved from the sources the fraudster could not edit.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE VENDOR THAT SHARED A SORT CODE

An FD's routine analytics flagged a facilities vendor with invoices always just under the second-signature threshold. The covert phase preserved before anyone asked questions: vendor-master logs, the procurement manager's mailbox and phone-eligible chat, approval records. The joins did the rest: the vendor created by the manager's own account on a Saturday; its bank details matching a beneficiary on his personal standing orders (the §8 counterparty layer, reached later under order); invoice PDFs whose authoring metadata named his home machine's user profile (guide 87); and a messaging thread with the "vendor's" director: his brother-in-law: scheduling invoice submissions around approval-cover gaps. The transaction schedule reached £412,000 over three years. Civil recovery ran on a freezing order supported by the examiner's affidavit; the criminal referral followed judgment, by design (§7's sequencing). The fraud was ordinary; the case was the joins.

EXAMPLE 2 · THE COVENANT CERTIFICATE BUILT IN ONE EVENING

A lender's suspicions about a borrower's covenant compliance became a claim when the certified management accounts diverged from insolvency-stage reality. The §6 examination of the certified spreadsheet was decisive: the workbook's session evidence showed every "monthly" tab created in a single four-hour sitting eleven days before the certificate date; the version ladder in the borrower's own DMS held the genuine monthlies: materially worse: superseded by the rebuilt file; and the CFO's mailbox carried the thread: "rebuild the pack so the ratios clear, keep the old one off the system": which guide 95's analysis showed had been followed by deletion attempts the DMS versioning survived. The authenticity report, graded and alternative-addressed per §6, anchored both the misrepresentation claim and the auditors' regulatory notifications. Documents remember how they were made; certificates are documents.

EXAMPLE 3 · THE MANDATE CHANGE NOBODY VERIFIED

A construction group paid £780,000 against a genuine subcontractor's "updated bank details", received by email. The investigation split cleanly along §3's diversion map: the request came from a lookalike domain registered nineteen days earlier (guide 80's evidence: registrar, nameservers, the cousin-spelling), following a compromise of the subcontractor's real mailbox where a forwarding rule (guide 104) had been harvesting the payment conversation for a month; the group's own verification procedure: callback to a known number: existed on paper and was skipped under month-end pressure, per the AP clerk's honest interview and the absent call log. Deployment ran §7's full spread: bank-recall and receiving-institution engagement at fraud speed, insurer proof on the examiner's report, the subcontractor's own liability position negotiated on the shared forensic file, and process remediation both companies' auditors required. Attribution of the criminal end went to the referral; the civil allocation turned on the verification gap the estate documented precisely.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The premature question:** the suspect asked "to explain" before preservation: the estate swept by morning: §4's discipline inverted.
- **Report-level extraction:** ERP data taken as standard reports without audit tables: the who-and-when layer never collected.
- **Anomaly pleaded as fraud:** analytics findings deployed without the communications join or baselines: Example 3 of guide 97's lesson at corporate scale.
- **Privilege structured late:** the investigation's purpose file assembled at disclosure: guide 91 Example 2's fate for the whole file.
- **Single-track tunnel vision:** civil proceedings launched without weighing the criminal, regulatory and insurance interactions: §7's sequencing skipped, options foreclosed.
- **The counterparty layer ignored:** the fraudster's editable records treated as the whole truth: §8's unreachable sources never pursued.
- **Interviews before evidence:** accounts taken that the later forensics contradict or that contaminate recollection: the interview sequenced after the record, not before.
- **Quantification drift:** the schedule serving no audience well because it was built for none: §5's multi-audience design ignored.

Technical limitations

- **Audit depth varies:** ERP and platform logging differ by configuration and licence: the investigable story bounded by what was recorded, stated per source.
- **Cash and off-system steps:** value moving outside the estate (cash, third-party accounts, crypto per guide 128) needs the external routes: gaps named, not glossed.
- **Attribution ceilings:** accounts and devices attribute to hands only as far as guides 105-107 allow: shared credentials and delegated access stated as such.
- **Authenticity conclusions are graded:** §6's findings run from "inconsistent with the claimed date" to "fabricated": the report claims the supportable grade, and no more.
- **Covert reach has legal edges:** personal devices, private accounts and covert monitoring sit behind guide 97 §5's frame and §7's process: planned with advice, never improvised.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who is inside the need-to-know circle: and can preservation complete before anyone outside it senses the question?
- Which §3 scheme pattern fits the suspicion: so week one secures that pattern's signature artefacts first?
- Which audiences will need the findings: insurers, auditors, regulators, police: so privilege and sequencing are designed now?

Ask your opponent (in ensuing proceedings)

- Please disclose the audit and change-history records of [the financial system] for [the relevant vendors / journals / periods], including user, timestamp and prior-value data, and confirm the system's audit configuration during the period.
- Please disclose all versions and drafts of [the questioned document], the stores in which each resided, and the transmission records by which it was communicated on or about its stated date.
- Please confirm preservation of the mailboxes, messaging accounts and devices of [named individuals], including any personal accounts used for company business, pending determination of the disclosure applications.

Ask your eDiscovery / forensic provider

- Is the covert phase's preservation complete across the §3 map: and what remains exposed if the suspect learns tomorrow?
- Do the joins hold: transaction to communication to hand: at the grade the pleading needs?
- What does the §6 authenticity work support: and what alternative explanations has it addressed?

SUGGESTED WORDING · INSTRUCTION FOR A FRAUD INVESTIGATION

> "You are instructed, on a strictly confidential basis and under the direction of [instructing solicitors] in contemplation of litigation, to: (1) preserve, by means not visible to the individuals named in Schedule 1, the data sources listed in Schedule 2 [mailboxes, drives, messaging, devices, financial-system audit records and logs]; (2) examine the preserved material for evidence of [the suspected scheme], including correlation of financial-system records with communications and document-authenticity examination of the items in Schedule 3; (3) attribute relevant actions to individuals so far as the evidence permits, stating the basis and limits of attribution; (4) prepare a transaction schedule quantifying the suspected loss with evidence references; and (5) report in a form suitable for exhibition under CPR Part 35, identifying findings, alternative explanations considered, and the confidence attaching to each conclusion. All work is to maintain chain of custody and comply with UK GDPR, with the methodology documented throughout."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The fraud-investigation checklist

- ☐ Need-to-know circle defined; leak surface minimised
- ☐ Privilege structure and purpose file set at instruction
- ☐ Covert preservation complete across the §3 pattern's sources
- ☐ Audit logs and perishables exported inside their windows
- ☐ Financial systems extracted forensically, audit tables included
- ☐ Analytics run as lead generation; baselines respected
- ☐ Communications joins built on guide 96's frame
- ☐ Questioned documents examined per §6; conclusions graded
- ☐ Counterparty and registry layers pursued for the unreachable record
- ☐ Deployment sequenced across civil, criminal, regulatory, insurance

Red flags

- Vendors created or edited by the accounts they pay: Example 1's Saturday.
- Certificates and packs built in single sessions near their dates: Example 2's evening.
- Mandate changes without completed verification callbacks: Example 3's gap.
- Approval chains routed around their designed steps.
- The unofficial channel carrying what the file omits.
- Deletion and wiping clustered at audit or dispute dates: guides 95 and 110.
- Lookalike domains registered weeks before payment events: guide 80's calendar.

When to involve a digital forensic expert

At first suspicion, before any question is asked aloud: the covert phase is designed, not improvised, and §4's window closes on contact; through examination, where the extractions, joins, attributions and authenticity work are built to the grade the gravest allegation needs; and at deployment, where affidavits support freezing and search relief, reports run under CPR Part 35, and referral bundles meet criminal-evidence expectations: with guide 100's instruction disciplines governing the expert relationship throughout. Through **cflab.uk** and **e-discovery.uk**, fraud work runs from the quiet fortnight to the courtroom as one engineered engagement: and the quiet fortnight is only available once.

§ 13 · COMMON QUESTIONS

Frequently asked questions

We suspect fraud but are not certain. Should we investigate before involving lawyers?

Involve them first: the privilege structure (§7) only protects an investigation built inside it, and the covert phase (§4) needs legal design around monitoring, scope and employment risk: informal look-arounds spend both protections and often tip the suspect: guide 97 Example 2 at higher stakes. Suspicion is exactly the moment the structure is cheap.

How do we investigate without the suspect finding out?

Server-side: holds, log exports and admin-level preservation invisible to users (§4), device work inside routine cover where lawful, and a need-to-know circle small enough to hold: most tip-offs are internal and accidental. The phase ends deliberately, with confrontation timed after preservation and with guide 97's letters ready for the personal estates.

Can forensics really prove a document was backdated or fabricated?

Frequently, from internal evidence: authoring artefacts against the claimed date, session and save-count patterns, resource anachronisms, absent transmission records and surviving true versions (§6, guides 87 and 109): Example 2's certificate is the standard demonstration: with conclusions graded to what the artefacts support. The strongest cases pair the internal evidence with the counterparty's clean copy.

Should we report to the police, and when?

Weigh it with advice (§7): referral can stay civil proceedings, affect insurance and regulatory positions, and remove control of tempo: while some duties and policy terms require or reward early report: the decision is strategic and matter-specific. What the forensic file guarantees is that whichever order is chosen, the evidence is ready for both standards.

The books themselves may be doctored. What can we trust?

The §8 matrix's unreachable layer: bank records against the ledger, counterparties' copies against the file, registries against the backdated agreement, platform audit tables against the edited entries: fraudsters falsify what they control, and the investigation is built on what they could not reach. A doctored system is not a dead end; it is an authenticity exhibit.

How fast can freezing-order evidence be ready?

Where the covert phase preserved well, the examiner's affidavit: the joins, the schedule, the dissipation indicators: can support an application in days: Example 1's pattern: with full-and-frank obligations shaping what is included, prominently including the alternative explanations addressed. Speed is a preservation dividend: it is earned in the quiet fortnight, not the application week.

§ 14 · REFERENCE

Glossary

Approval-chain reconstruction
Tracing each authorisation to an account, then a hand.

Audit tables
A financial system's own record of who changed what, when.

Covert phase
Preservation and examination before suspects learn of the inquiry.

Freezing injunction
The order restraining dissipation of assets pending claim.

Journal-entry testing
Pattern analysis of postings for manipulation signatures.

Mandate fraud
Payment diversion via false bank-detail change requests.

Need-to-know circle
The restricted group aware the investigation exists.

Transaction schedule
The evidenced, quantified list of suspect payments.

Vendor-master
The supplier database whose change logs date fraud setup.

Version ladder
The surviving true history bracketing a questioned document.

Sources and authoritative references

The fraud-investigation disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (fraud examination, authenticity testing, covert preservation, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 07 · Analysis (holds, extraction and the joins as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/analysis
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- CPR Part 25 (freezing injunctions and search orders): justice.gov.uk, Part 25 · CPR Part 35: justice.gov.uk, Part 35 · PD 57AD: justice.gov.uk, PD 57AD
- Fraud Act 2006: legislation.gov.uk, Fraud Act 2006 · Action Fraud (reporting): actionfraud.police.uk · SFO: sfo.gov.uk
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Fraud engagements at the laboratory are built around the two clocks that matter: the covert window and the remedies timetable. Week one secures the §3 pattern's signature sources server-side and silently; the examination then runs the compounding disciplines: forensic financial extraction with audit tables, the communications joins on guide 96's frame, attribution to guide 105-107 standards, and §6's authenticity work with graded conclusions and alternatives addressed: while the transaction schedule is engineered once for every audience the matter will meet. Affidavits support freezing and search applications at the speed Example 1 describes; reports run under CPR Part 35; referral bundles are packaged to criminal-evidence expectations; and the same rigour serves respondents, because the innocent explanation found early (guide 97 Example 3's principle) is worth more than the dramatic one found late. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if the suspicion is live today, the covert window is open today: it does not reopen.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace