SAMPLE PRE-ACTION DIGITAL EVIDENCE TRIAGE WORKPAPER (100% SYNTHETIC)

Matter Reference: `SYN-PILOT-2025-0100` *(100% Clean-Room Specification Scenario — Zero Real Client Data)*
Scenario Type: UK Micro-Enterprise Domestic Faster Payments Supplier Invoice Diversion (`PSR Specific Direction 20` Scope)
Prepared By: Ziqi Xiao (`starshield-forensics v0.3.6` Deterministic Triage Workflow)
Engagement Basis: Pre-Action Technical Consultancy Workpaper for Instructing Solicitors *(Fixed-Fee Tier, Non-Contingent; Not a CPR Part 35 Report)*
Document Classification: `TLP:CLEAR — Reproducible Synthetic Sample Deliverable`

1. Executive Summary & Scope of Instructions

1. **Fictional Fact Pattern:** On `18 March 2025` (post- `7 October 2024` implementation of mandatory APP reimbursement under **PSR Specific Direction 20**, para 3.2), a fictional UK micro-enterprise (*"Example-Co Precision Synthetic Ltd"*, 6 employees, annual turnover `£620k` — qualifying as a protected micro-enterprise) remitted **`GBP 18,400.00` via UK Faster Payments** (within the `£85,000` PS24/7 regulatory maximum reimbursement level) after receiving amended domestic settlement details inside a browser-based procurement portal thread impersonating its regular UK component vendor. Ten minutes after composition, the impersonator soft-deleted the payment instruction (`"This message was deleted"` in UI screenshots) and sent a follow-up reserve cross-border IBAN/card demand (`msg_spec_0002`), which was halted unpaid.
2. **Scope of Technical Triage:** Instructed on a synthetic demonstration basis to: (a) inspect a consented, read-only copy of the Chromium `IndexedDB` write-ahead log (`000003.log`) and exported JSON archive (`synthetic_case_benchmark.json`) to recover soft-deleted records prior to LevelDB compaction; (b) validate extracted banking identifiers via deterministic ISO/IEC 7812 Luhn, ISO 13616 IBAN Mod-97, and ISO 9362 BIC rules; (c) inspect RFC 2083 PNG container metadata on a disputed "Stamped Bank Audit Notice"; and (d) compile an offset-cited schedule for solicitor review.

2. Reproducible Chain-of-Custody & Read-Only Acquisition Manifest

(Every byte length, `SHA-256` digest, and byte offset below matches the deterministic `starshield-forensics v0.3.6` specification vectors 1-to-1.)

Exhibit ID	Synthetic Specification Vector	Exact Byte Length	Reproducible SHA-256 Digest	Verification Module
EXH-01	`build_synthetic_leveldb_wal_bytes()` (`000003.log`)	`68,779 B`	`c2ac19e91535c2a641023ac96893c2d5c25a38c3e5f507254e91e75bf6b172ff`	`leveldb_wal_32k_crc32c_v0.3.6`
EXH-02	`samples/synthetic_case_benchmark.json`	`2,570 B`	`a2a722157007057ee1eb9de5a01b89c1c5080a36fc9ab433c97387aa3321e7b2`	`triage_exported_chats vc_json`
EXH-03	`build_valid_png_with_iccp("Display P3", "APPL", ...)`	`195 B`	`068e9a47ee0f1444b22b04bd151a9c5cae57b90ab8f43e4a1c256c2106aea2bf`	`inspect_image_container (RFC 2083)`

> **Provenance Caveat:** Cryptographic `SHA-256` digests attest post-acquisition byte integrity only. Upstream workstation custody and absence of prior LevelDB compaction depend on the client intake log recorded at acquisition.

3. Recovered Soft-Deleted Cache Records & Checksum-Validated Indicators

Parsing `EXH-01` across three `32,768` -byte LevelDB blocks (`FULL` + `FIRST` / `MIDDLE` / `LAST` reassembly; `4` valid physical frames; `0` Castagnoli `CRC32C` errors) recovered two soft-deleted WriteBatch JSON records hidden in UI views by `properties.deletetime` :

Seq #	Physical WAL Byte Offset	Message ID	Compose UTC / Soft-Delete UTC	Verbatim Cached UTF-8 Payload (`OBSERVED`)	Checksum-Validated IOCs (`DERIVED`)	Epistemic Tier
`1001`	`0x00000000`	`msg_spec_0001`	`2025-03-18 10:00:00Z` Deleted: `2025-03-18 10:10:00Z`	`"Updated UK Faster Payments supplier account for Invoice INV-2025-0100 (GBP 18,400.00): Sort Code 00-00-00 Account 00000000."`	UK Sort Code `00-00-00` paired within 120-char window to 8-digit account `00000000` *(test vector)*	`OBSERVED` (Bytes) `DERIVED` (Pairing)
`1002`	`0x0000018D` *(3-block span)*	`msg_spec_0002`	`2025-03-18 14:30:00Z` Deleted: `2025-03-18 14:40:00Z`	`"Secondary reserve IBAN GB82WEST12345698765432 (SWIFT NWBKGB2LXXX), Norway test IBAN NO9386011117947, and Luhn test card 6200000000000005."`	• IBANs `GB82...` (len 22) & `NO93...` (len 15): **Mod-97 PASS** • BIC `NWBKGB2LXXX` : **ISO-3166 PASS** • Card `6200...0005` : **Luhn PASS**	`OBSERVED` (Bytes) `DERIVED` (Mod-97 / Luhn)

4. Disputed Container Provenance & PSR Specific Direction 20 Schedule

4.1 Structural PNG Container Inspection (`EXH-03` — `remittance_stamp_2025.png`)

- **Observed Structure (`OBSERVED` / `DERIVED`):** Valid 8-byte RFC 2083 PNG magic, `IHDR` (`1 x 1` minimal spec vector at offset `8`), `iCCP` chunk at byte offset `33` (`CRC32` valid) decompressing to a 160-byte ISO 15076-1 `acsp` profile (`Primary Platform: APPL` ,

`Description: Display P3`), `tEXt` chunk at byte offset `111` (`Software\x00QuickShot Raster Editor 4.2`), `IDAT`, and terminal `IEND`.

- **Mandatory Alternative Explanations:** Apple `Display P3` profiles and raster editor `tEXt` tags show consumer/raster pipeline export rather than native banking host PDF generation. Because staff occasionally screenshot legitimate PDFs on macOS/iOS, this is reported strictly as a **corroborative provenance discrepancy (`DERIVED`)**, never standalone proof of forgery.

4.2 Chronological Alignment for UK Faster Payments Reimbursement (`PSR Specific Direction 20`)

Under **PSR Specific Direction 20** and **Pay.UK FPS Reimbursement Rules** (applicable to eligible **UK Faster Payments** executed on or after `7 October 2024` by consumers, micro-enterprises, or small charities with annual income `<£1m` to a **"recipient account not controlled by the consumer"**), the schedule isolates objective evidence addressing PSP *"Consumer Standard of Caution"* objections:

UTC Timestamp (`2025-03-18`)	Source Exhibit & Offset	Objective Technical Observation	Relevance to Solicitor's PSR SD20 / FOS Submission
`10:00:00Z`	`EXH-01` (`offset 0x00000000`)	`msg_spec_0001` delivers UK Sort Code `00-00-00 / 00000000` inside existing supplier thread.	Reconstructs contemporaneous inducement text deleted from UI screenshots prior to claim intake.
`10:00:45Z`	`EXH-02` (`timestamp_pairs[0]`)	Disputed PNG audit notice (`EXH-03`, raster `tEXt` offset `111`) acknowledged (`+45.0s` UTC delta).	Corroborates active social-engineering artefact presented before Faster Payments authorization.
`10:06:18Z`	Claimant Bank Statement	Outbound UK Faster Payment (`GBP 18,400.00`) debited to third-party UK recipient account.	Post-`7 Oct 2024` UK Faster Payment within **PSR SD20** scope; recipient account not controlled by claimant.
`14:30:00Z`	`EXH-01` (`offset 0x0000018D`)	Unpaid follow-up `msg_spec_0002` adds cross-border `NO93...` IBAN & card rail; retracted at `14:40:00Z`.	Cross-border SEPA/card rails fall outside FPS SD20 reimbursement scope, while corroborating third-party fraudster control.

5. Quality Assurance Log & Methodological Boundaries

1. **Cache Compaction Boundary:** LevelDB background compaction purges overwritten entries; absence of earlier deleted records in `EXH-01` does not prove no prior retractions occurred.
2. **Sort-Code Weighting:** Validates Luhn, ISO-13616 Mod-97 (89 country lengths), and ISO-9362 BICs deterministically; UK Sort Code pairing uses a 120-char intra-message window without proprietary Vocalink modulus tables.
3. **Offline Execution & QA Sign-Off:** Stdlib-only Python >= 3.10 (`zero network calls`, `zero LLM uploads`, single-file `starshield.pyz` included); regression suite **`24/24` passed**; all digests and offsets verified directly against `starshield-forensics v0.3.6` (`DOI: 10.5281/zenodo.24145804`).