

PUBLIC SAMPLE / FICTIONAL ENGAGEMENT

Cybercrime investigation findings

Prepared for Northline Studio

A fictional organization used solely to demonstrate reporting. No client information, live indicators or actual evidence is included.

Report reference	Reporting cutoff	Intended reader
INV-001	07 Oct 2026 / 23:59 UTC	Authorized business representative and appointed counsel

EXECUTIVE ASSESSMENT

A fictional supplier-payment incident includes a changed payment instruction, a client-reported transfer and a lookalike sender reference. The reviewed copies support that the payment instruction changed, but not who changed it or who controlled the recipient account. The transfer amount is reported as USD 18,400; bank-confirmed loss and recovery are unknown.

DECISION REQUESTED

Have the authorized client contact its bank's fraud channel promptly and ask counsel to determine reporting and preservation obligations. Preserve originals before further analysis; avoid contact with the suspected sender.

Inside this report

02 Scope and method / 03 Findings / 04 Evidence and chronology / 05 Action plan / 06 Handover and limitations

Illustrative format only. Final scope, response cadence, authorized recipients and local requirements are agreed for each engagement. No service outcome or legal determination is promised.

02 / HALDEN INTELLIGENCE

Scope, coverage & method

AGREED QUESTION AND COVERAGE

Organize three supplied records, construct a qualified chronology and assess two hypotheses: unauthorized mailbox access versus an external lookalike communication. Authority is limited to client-owned materials voluntarily provided for the fictional matter.

OUTSIDE THIS ASSESSMENT

Bank account access, tracing private subscribers without lawful process, recovery of funds, actor engagement, payment to intermediaries, seizure, device acquisition and attribution to a real person.

Asset / record	Accountable owner	Coverage
AS-01 / Invoice thread	Finance owner	Supplied copies; original message export outstanding
AS-02 / Transfer record	Finance owner	Client-reported payment; bank confirmation pending
AS-03 / Supplier baseline	Procurement owner	Previous approved payment instruction

REPORTING METHOD

Define authority and scope; register supplied material; separate direct observations from statements; assess alternative explanations; review findings against source limitations; assign actions with acceptance evidence.

CONFIDENCE IS NOT SEVERITY

High: the cited material directly supports this narrow observation. Moderate: the observation has support but an important gap remains. Low: it is a lead or statement requiring corroboration. Confidence never establishes identity, intent or legal liability.

PRIORITY AND TIME

High: address promptly because of potential material harm or dependency. Medium: assign a near-term owner. Low: review in the agreed cycle. These are qualitative priorities, not CVSS ratings. All times are UTC; event times and receipt times are distinct.

03 / HALDEN INTELLIGENCE

Findings & interpretation

F-01 / HIGH PRIORITY / HIGH CONFIDENCE

Payment destination differs from the approved baseline

Observation. The fictional amended instruction and the earlier approved baseline show different masked recipient references.

Why it matters. The change is consistent with a payment-diversion scenario and warrants bank-led review.

Alternative / uncertainty. A legitimate supplier change remains possible until verified through a previously trusted independent channel.

Recommended action. The client should contact its bank and verify the supplier using an established contact, not the details in the disputed message.

Evidence: E-01, E-03

F-02 / HIGH PRIORITY / MODERATE CONFIDENCE

Lookalike sender does not prove mailbox compromise

Observation. The supplied screen view shows a near-match sender domain. Full original headers and authorized mailbox logs were not provided.

Why it matters. Containment and reporting decisions depend on whether the client's mailbox was accessed or merely imitated.

Alternative / uncertainty. Display-name spoofing, forwarding artifacts or a screenshot transcription error could alter interpretation.

Recommended action. Request an authorized original message export through the evidence channel and ask the appointed responder to assess mailbox access.

Evidence: E-01

F-03 / MEDIUM PRIORITY / LOW CONFIDENCE

Loss and beneficiary control are not independently established

Observation. A supplied transfer screenshot states USD 18,400. It does not establish settlement, recall status, beneficiary identity or ultimate control of funds.

Why it matters. Reporting the amount as a confirmed unrecoverable loss would overstate the available evidence.

Alternative / uncertainty. The transfer could be held, reversed, misrecorded or legitimately instructed.

Recommended action. Record bank-confirmed status separately from the client's account and avoid identity claims without lawful supporting evidence.

Evidence: E-02

04 / HALDEN INTELLIGENCE

Evidence & chronology

Evidence register

ID / source	Receipt time (UTC)	Known limitation
E-01 / Fictional changed-instruction screen copy	2026-10-03 10:10 UTC	Original message and headers missing
E-02 / Fictional masked transfer screenshot	2026-10-03 10:15 UTC	Not a bank attestation; amount is client reported
E-03 / Fictional prior supplier instruction	2026-10-03 11:00 UTC	Supplied baseline; supplier verification pending

Event chronology

Event time (UTC)	Recorded event	Source
02 Oct / 14:20	Changed instruction time shown in copy	E-01; source clock unverified
02 Oct / 15:05	Transfer time displayed in screenshot	E-02; bank confirmation pending
03 Oct / 11:00	Baseline compared; discrepancy documented	E-03

HANDLING AND PROVENANCE

The entries above are invented descriptions, not evidence attachments. In a real engagement, assign a unique evidence ID; record collector, authority, source, collection and receipt times, method and limitations; retain the original in approved storage; and log access, transformations and transfers. Calculate digests on actual files where appropriate. Never invent a digest or custody event.

SOURCE BOUNDARIES

A screenshot can support what was visible in that copy. It does not, on its own, prove origin, completeness, authorship or the full history of an event. Preserve contradictions and distinguish client-reported events from independently verified observations.

05 / HALDEN INTELLIGENCE

Action plan & service register

When	Owner	Completion evidence	State
Promptly	Authorized finance owner	Contact bank fraud team and retain reference	Client action
Before further analysis	Evidence custodian	Preserve original message and supplied files	Open
Within agreed scope	Appointed responder	Assess authorized mailbox logs and alternative hypotheses	Referred
Before external disclosure	Client counsel	Approve recipients and disclosure basis	Required

Hypothesis assessment

Hypothesis	Supporting / contrary evidence	What would change assessment
External impersonation	Near-match sender supports; original unavailable	Original headers and trusted supplier verification
Mailbox compromise	No direct access evidence supplied	Authorized identity/mailbox event review
Legitimate payment change	Not excluded by copies alone	Independent supplier confirmation and bank record

These hypotheses are not mutually exclusive. This report identifies evidence gaps, not a suspect or a recovery probability.

CLOSING AN ACTION

Record the actual completion time, responsible person and evidence reference. A request, recommendation or platform submission is not completion. Keep unresolved dependencies visible and agree the next review date with the client.

Limitations & handover

LIMITS ON RELIANCE

Copies may omit context or metadata. Timestamp accuracy is not independently verified. This is technical support, not legal advice or a promise of identification, funds recovery or admissibility.

DISTRIBUTION AND RETENTION

This fictional sample is public. A live report requires an approved recipient list, secure delivery method, retention schedule and disposal owner agreed with the client and, where relevant, counsel. Do not place real evidence or personal data in public website assets.

Release checklist for a live engagement

Required check	Record to complete before issue
Authority and scope	Approved instruction reference and authorized assets
Analyst and peer review	Named preparer, reviewer, review date and corrections
Client decisions	Decision owner, accepted actions and unresolved objections
Delivery and acceptance	Approved recipients, transfer receipt and acceptance date
Follow-up and retention	Next review, retention basis and disposal responsibility

These fields are deliberately unsigned. No real review, instruction, client approval or evidence transfer is represented by this sample.

Method references

Background guidance only; these publications do not validate fictional findings or certify this report. Apply current platform procedures and engagement-specific legal advice separately.

NIST SP 800-86 — Guide to Integrating Forensic Techniques into Incident Response (2006)
<https://csrc.nist.gov/pubs/sp/800/86/final>

NIST SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management (2025)
<https://csrc.nist.gov/pubs/sp/800/61/r3/final>