FINANCIAL CRIMES

Case Name:	Shell Company Offshore Movement
Case Number:	Sample Use Case
Report:	Financial SITREP Use Case
Report Date:	Aug. 30 2026
Report Span:	Sample Scenario

Shell Companies Move $14.2M Through Pass-Through Accounts and Offshore Entities

A Financial SITREP helps investigators quickly understand whether a set of suspicious transfers is an isolated fraud, a laundering structure, offshore profit movement, sanctions exposure, or part of a broader organized financial-crimes pattern.

What Happened

Federal investigators receive a referral after a corporate audit, bank alert, and customer complaint point to the same problem: money that should have remained inside normal commercial payment channels moved through newly formed entities, domestic pass-through accounts, payment processors, and offshore destinations. Several entities appear legitimate on paper, but their formation dates, bank details, invoice descriptions, and transfer timing do not match the normal business purpose of the payments.

The referring bank's financial-crimes unit completed the first review and identified unusual wires, repeated settlement references, and several receiving accounts tied to newly created companies. The corporate victim provided NetSuite exports, invoice records, vendor master files, approval logs, contract documents, and payment histories. Payment processors provided payout records, refund activity, account identifiers, and settlement reports. No single source showed the full path from the original payments to the offshore movement.

The early investigative question is not simply whether money moved. The question is what kind of case this is: vendor fraud, shell-company laundering, insider-enabled diversion, offshore profit dumping, tax evasion, sanctions exposure, corruption, or a larger financial-crimes network.

Size and Scope

The response team saved available financial records into a ZIP file and imported them into REMI. REMI identified **82 flagged transactions** across **nine domestic entities**, **five offshore entities**, **six bank accounts**, **three payment processors**, and **four vendor records**. The preliminary amount at issue was **$14.2 million**, including **$9.6 million confirmed as transferred offshore**, **$2.1 million moved through domestic pass-through accounts**, **$1.3 million tied to processor payouts or refunds**, and **$1.2 million unresolved pending bank and beneficial-owner records**.

The strongest relationship set involved **HarborLight Trading LLC**, **Blue Meridian Consulting Ltd.**, receiving account ending **2197**, offshore account ending **7714**, payment references **HLT-77xx**, and repeated approvals by **r.ellis@company.example**. The first supported suspicious event appeared on **April 4 at 09:18 UTC**, when a new vendor profile was created using contact details later reused by two other entities.

Within 11 days, REMI found a pattern of invoice creation, approval, domestic account deposits, split transfers, processor payouts, and offshore wires. The activity crossed multiple systems and would have been difficult to reconstruct from any one ledger, bank statement, processor file, or vendor record alone.

What REMI Connected

REMI connected entity names, bank accounts, routing details, invoice numbers, payment references, approver accounts, formation dates, processor settlement IDs, wire timestamps, IP addresses, mailing addresses, and repeated contact information across separate records. Several entities used different names but shared bank details, registered-agent information, phone numbers, email patterns, or transaction references.

The SITREP showed that money moved from operating accounts into domestic shell or pass-through entities, then split into smaller transactions. Some funds moved through payment processors as payouts and refunds, some were layered through additional domestic accounts, and some were wired to offshore entities with unclear beneficial ownership.

Behaviors Identified

- Shell-entity formation followed by rapid payment activity
- Pass-through account behavior with limited business purpose
- Split transfers, layering, and circular movement
- Offshore wires to entities with unclear beneficial ownership
- Repeated bank details, addresses, contact data, and payment references across entities
- Invoices with generic descriptions and weak supporting documents
- Approvals outside expected workflow or timing patterns
- Processor payouts, refunds, and settlement records that obscure final destination
- Possible insider approval abuse, credential misuse, or vendor enablement requiring follow-up

What Remains Unresolved

The SITREP does not conclude who controlled the shell companies or whether every entity had criminal intent. The evidence supports that funds moved through related accounts and entities in a pattern consistent with layering and offshore movement. Additional records are needed to determine beneficial ownership, whether an insider approved or enabled the payments, whether the entities share control, whether the offshore destinations are tied to tax evasion or sanctions exposure, and whether the movement is part of a broader organized financial-crimes structure.

Time Saved in the First Hours

Without a unified review, the team would likely spend days building the first entity map and transaction timeline from bank records, ledgers, invoices, processor exports, vendor files, and offshore account references. Early delays matter because financial records can be amended, accounts can be closed, funds can be moved again, and key context can be lost before subpoenas or preservation requests are issued.

By importing the available records into REMI, investigators receive an early Financial SITREP in minutes. The SITREP gives the team a working case map during the first hours: which transactions triggered flags, which entities appear connected, how money moved, what damages are known, which offshore paths need review, which evidence supports each finding, and what records should be preserved or requested first.

Sample Priority Next Steps

1. Preserve source financial exports	Preserve the original ledgers, bank statements, wire records, processor exports, invoices, vendor files, approval logs, and entity records used in the SITREP, including file hashes, timestamps, custodians, and export parameters.
2. Subpoena domestic receiving accounts	Request complete records for receiving account ending 2197 and related domestic accounts, including account opening documents, beneficial-owner information, authorized signers, linked accounts, deposits, wires, ACH activity, withdrawals, and communications.
3. Trace offshore wires	Trace the wires to offshore account ending 7714 and related entities, including correspondent banks, intermediary routing, destination institutions, reference fields, and any partial returns or onward movement.
4. Identify beneficial owners	Collect beneficial-owner records, incorporation documents, registered-agent details, tax identifiers, signatory records, mailing addresses, phone numbers, and email addresses for HarborLight Trading LLC, Blue Meridian Consulting Ltd., and related entities.
5. Review shared identifiers	Compare reused bank accounts, routing numbers, payment references, addresses, phone numbers, email domains, IP addresses, approvers, and settlement IDs across all flagged entities and transactions.
6. Review approver and insider access	Review activity for r.ellis@company.example and other approvers, including login history, MFA events, device fingerprints, approval timestamps, normal workflow patterns, and whether any user had authority to create or approve the flagged vendors.
7. Validate invoice legitimacy	Compare HLT-77xx invoice records against contracts, purchase orders, receiving documents, delivery records, vendor history, and prior payment patterns to identify unsupported billing or fabricated business purpose.
8. Analyze processor payouts and refunds	Request full processor records for payouts, refunds, chargebacks, settlement batches, linked bank accounts, account owners, device/IP data, and destination accounts tied to the flagged transactions.
9. Evaluate AML, sanctions, tax, and corruption exposure	Screen connected entities, jurisdictions, beneficial owners, counterparties, offshore destinations, transaction paths, and business purposes for AML red flags, sanctions concerns, tax-evasion indicators, bribery, corruption, or organized financial-crime patterns.
10. Prepare targeted interviews and document requests	Prepare questions for bank personnel, corporate accounting staff, approvers, vendor contacts, registered agents, payment processors, and entity representatives based on unresolved SITREP findings.

See the REMI workbook for supporting detail, including account numbers, transaction IDs, entity names, beneficial-owner indicators, vendor records, approver activity, timestamps, IP addresses, source records, damages calculations, relationship maps, offshore transfer paths, and the evidence links used to support each finding.