FINANCIAL CRIMES

Case Name: ABC Bank Vendor Payment Fraud
Case Number: Sample Use Case
Report: Financial SITREP Use Case
Report Date: Aug. 30 2026
Report Span: Sample Scenario

ABC Bank Escalates $8.7M Vendor Payment Fraud to Federal Investigators

A Financial SITREP helps investigators understand the size, scope, damages, connections, behaviors, unresolved questions, and priority next steps during the first hours of a serious financial-crimes response.

What Happened

A regional bank's fraud operations team received complaints from multiple commercial customers that approved vendor payments had not reached the intended vendors. The customers reported that invoices appeared legitimate, approvals were recorded in their accounting systems, and payments were released through normal banking channels.

The bank's internal fraud team performed the first review and found that several vendor-payment instructions had been changed shortly before large payments were released. The affected customers provided ledger exports, vendor files, invoice records, approval logs, and payment histories. The bank provided account-change records, wire activity, receiving-account details, customer complaint records, and available IP logs.

Because the records were spread across the bank, customer accounting systems, payment processors, vendor documents, and transaction histories, investigators did not yet have one clear timeline of how the money moved or whether the matter involved account takeover, vendor fraud, insider approval abuse, shell companies, or money laundering.

Size and Scope

The response team imported the available records into REMI to quickly size the case. REMI identified **47 flagged transactions** across **14 commercial customers**, with estimated exposure of **$8.7 million**. Of that amount, **$6.1 million was confirmed as transferred**, **$1.4 million appeared partially returned or reversed**, and **$1.2 million remained unresolved** pending receiving-bank and payment-processor records.

The strongest relationship set involved **Northstar Supply LLC**, receiving account ending **8842**, approver account **m.harris@company.example**, invoice series **NS-44xx**, two outbound wires posted between **March 12 and March 14**, and later movement through three pass-through accounts and one offshore entity.

REMI found that the first supported suspicious event was a vendor-payment change recorded on **March 9 at 16:42 UTC**. That change replaced a previously known vendor account with a new receiving account. Within 24 hours, three invoices were entered, two approvals occurred outside the normal approval window, and the first wire was released.

What REMI Connected

REMI connected the vendor-account change to later invoices, approval events, wire transfers, payment references, receiving accounts, refund activity, and offshore movement. The same vendor name, invoice pattern, receiving account, approver account, and payment references appeared across separate records that had not previously been reviewed together.

The SITREP showed that funds moved from customer accounts into the substituted receiving account, then split into smaller transfers. Some funds moved through additional business accounts, some appeared in payment-processor settlement records, some were partially returned, and some were routed to an offshore entity with unclear beneficial ownership.

Behaviors Identified

- Vendor-payment diversion and vendor-account substitution
- Approval-policy bypass and unusual approval timing
- Split-transfer movement and pass-through account behavior
- Possible shell-company routing and offshore movement
- Partial return or reversal activity
- Incomplete or mismatched ledger descriptions
- Possible insider or credential misuse requiring follow-up

What Remains Unresolved

The SITREP did not conclude who committed the fraud. The evidence supports that payment instructions were changed and funds were diverted, but additional records are needed to determine whether the vendor was compromised, whether an employee knowingly assisted, whether credentials were stolen, whether the approver account was misused, and whether the offshore movement reflects money laundering, tax evasion, sanctions exposure, or another financial-crimes pattern.

Time Saved in the First Hours

Without a unified review, the team would likely spend the first several days manually comparing bank records, customer ledgers, invoices, payment processor exports, approval logs, and vendor records just to build the first timeline.

By importing the available records into REMI, investigators receive an early Financial SITREP in minutes. That gives the team a working case map during the first hours of the response: which transactions triggered flags, which customers were affected, how money moved, which accounts and entities are connected, what damages are known, what remains unresolved, and which records should be preserved or requested first.

Sample Priority Next Steps

1. Preserve vendor account-change records	Preserve all records showing the March 9 vendor-payment change for Northstar Supply LLC, including user account, timestamp, originating IP address, previous bank details, new bank details, approval history, and any supporting documents uploaded with the change.

2. Subpoena receiving-bank records	Request records for receiving account ending 8842, including account opening documents, beneficial-owner information, authorized signers, linked accounts, inbound deposits, outbound wires, ACH transfers, withdrawals, and communications related to the account.
3. Trace the split transfers	Trace the two outbound wires posted between March 12 and March 14 and identify all downstream accounts that received funds, including pass-through accounts, payment processors, offshore entities, refund paths, and partial returns.
4. Review approver activity	Review activity for m.harris@company.example, including login history, MFA events, device fingerprints, approval timestamps, normal approval patterns, and whether the account owner was present when the vendor change and invoices were approved.
5. Collect missing vendor communications	Collect emails, attachments, portal messages, support tickets, invoice submissions, and payment-change requests involving Northstar Supply LLC, affected customers, and any third-party payment contacts.
6. Compare invoices against vendor history	Compare invoice series NS-44xx against prior Northstar Supply LLC invoices to identify duplicate invoice numbers, abnormal amounts, changed remittance instructions, altered payment terms, unusual descriptions, or mismatched purchase orders.
7. Review possible insider involvement	Determine whether any employee, contractor, or vendor user had the access needed to create or approve the payment change. Review whether actions occurred during normal business hours, from expected locations, and from previously known devices.
8. Identify offshore entity links	Review the offshore entity receiving later funds for shared identifiers, including beneficial owners, mailing addresses, bank references, phone numbers, email addresses, registered agents, IP addresses, and transaction timing.
9. Evaluate AML, sanctions, and tax exposure	Screen connected entities, account holders, jurisdictions, counterparties, and transaction paths for AML red flags, sanctions concerns, tax-evasion indicators, corruption risk, and organized financial-crime patterns.
10. Prepare interview and document-request questions	Prepare targeted questions for the bank, affected customers, approvers, vendor contacts, and payment processors, including who requested the payment change, who approved it, who controlled the receiving account, and why funds moved through multiple accounts.

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