Hidden Door Case Study – Forensic Investigation Report

Title: Multi-Office Corporate Embezzlement Investigation – ₹15 Crores Revenue Impact

---

Abstract

This case study presents the results of a comprehensive forensic investigation led by Hidden Door into a suspected internal fraud involving ₹15 crores in a large Indian corporation. The multi-layered embezzlement scheme was perpetrated across two major metropolitan offices. Through the use of digital forensics, financial data analytics, and surveillance, the investigative team traced fraudulent transactions, identified key perpetrators, and facilitated the recovery of ₹12.5 crores. This study highlights the value of a structured, technology-driven approach to corporate fraud investigations.

---

1. Introduction

Corporate fraud represents a growing risk for organizations, particularly in environments with distributed operations and limited integration of oversight systems. In this case, the client—a confidential Indian corporation—sought an external investigative partner to uncover a suspected financial discrepancy.

---

2. Objectives

Objective ID	Objective Description
OBJ-01	Map structure and scope of suspected fraud
OBJ-02	Quantify financial damage
OBJ-03	Identify involved personnel and external actors
OBJ-04	Recover funds and recommend preventive controls

Objective ID	Objective Description
OBJ-05	Compile legal-grade documentation to support disciplinary actions

---

3. Methodology

3.1 Investigation Duration and Scope

Metric	Description
Investigation Duration	4 months
Geographic Scope	Delhi and Mumbai offices
Departments Involved	Finance, Procurement, Operations
Employees Reviewed	87
Vendor Transactions Analyzed	12,300+

3.2 Tools and Technologies Used

Technology / Tool	Purpose
FTK Imager, Autopsy	Disk imaging and forensic data recovery
Cellebrite UFED	Mobile phone and encrypted message extraction
Maltego, IBM i2 Analyst's Notebook	Network link analysis of internal-external connections
Python (Pandas, NumPy)	Financial pattern analysis
Microsoft Power BI	Visual analytics and anomaly detection

---

4. Investigative Approach

4.1 Digital Forensics

- Captured forensic images of 53 laptops and 17 desktops.
- Recovered 430 deleted files including forged invoices and communication logs.
- Traced communication between employees and shell vendors using encrypted channels.

4.2 Financial Analytics

- Detected fund siphoning patterns across 3 fiscal quarters.
- Identified 27 suspicious vendors submitting repetitive low-value invoices.
- Created a fraud probability matrix using scoring heuristics.

Sample Financial Anomaly Table:

Invoice ID	Vendor Code	Amount (₹)	Flagged Issue	Approval Source
INV-2021	VND-M04	4,72,000	Duplicate Service Entry	Internal PO
INV-3339	VND-D12	9,10,000	No Supporting Document	Bypassed Tier-2
INV-3401	VND-M07	6,25,000	Forged Signature	Tier-1

4.3 Surveillance & Human Intelligence

- Deployed static surveillance outside vendor premises.
- Collected voice recordings indicating collusion.
- Conducted 14 anonymous staff interviews and exit route tracing for 3 resigning employees.

---

5. Key Findings

5.1 Fraud Architecture

- Fraudulent activities were distributed across two cities to evade audit trails.
- Use of dummy vendor firms with rotating invoice cycles and disguised billing codes.
- A collusion ring of 7 employees coordinated invoice creation, approval, and fund transfer.

5.2 Geographic Disparity

Region	Role in Fraud
Delhi	Document authorization and approvals
Mumbai	Bank routing and cash extraction

5.3 Organizational Failures

- Lack of multi-level invoice authentication.
- Absence of vendor legitimacy verification.
- Compartmentalized finance operations with limited cross-auditing.

---

6. Recovery and Legal Outcomes

6.1 Financial Recovery

Method	Amount Recovered (₹)
Bank Freezes	6.4 crores
Negotiated Settlements	3.1 crores
Asset Seizures	2.3 crores
Total	**₹12.5 crores**

6.2 Disciplinary Action

- Termination of 7 staff.
- Blacklisting of 19 vendors.
- Submission of 200+ page dossier to client's legal team.

---

7. Recommendations

7.1 Policy & Process Changes

Recommendation	Description
Centralized Vendor Onboarding	Mandated background checks via third-party KYC services
Multi-layer Invoice Approvals	AI-enabled invoice review thresholds
Real-time Financial Anomaly Detection	Integration of rule-based flagging with ERP systems
Anonymous Reporting Channels	Implementation of secure, reward-based whistleblower systems

7.2 Strategic Controls

- Implement quarterly forensic audits.
- Introduce rotating finance assignments to reduce collusion risk.
- Enforce device monitoring for high-risk personnel.

---

8. Conclusion

This investigation exemplifies a successful, technology-augmented fraud resolution strategy within a high-value corporate environment. Hidden Door's integrated approach enabled the client to recover a significant portion of misappropriated funds while also reinforcing future fraud defenses.

Project Leadership

This investigation was led by:

- **Haren Sarma**, Senior Forensic Consultant, Hidden Door
- **Ananya Joshi**, Cyber Intelligence Analyst, Hidden Door

Their leadership and cross-functional coordination were instrumental in delivering a timely and effective resolution.

Prepared by: Hidden Door Intelligence Team
Classification: Confidential – Hence no date or company name is mentioned.