EXECUTIVE BRIEFING: AI-Powered Fraud Forensic Engine

Overview

Traditional fraud detection focuses on "stopping the transaction." Our **AI Fraud Investigator** focuses on "identifying the source." It is a specialised forensic engine designed to analyse complex incident reports, stakeholder statements, and system logs to pinpoint whether a fraud is external or an insider threat.

The Problem: The "Silent Insider"

Financial institutions lose billions annually to internal fraud that goes undetected because:

- **Manual Audits are Slow:** Investigations take weeks, allowing the perpetrator to hide tracks.
- **Investigative Bias:** Internal relationships often cloud the objectivity of the Special Investigations Unit (SIU).
- **Process Gaps:** Institutions often flag the fraud but fail to identify which specific internal process was compromised.

The Solution: Deep Forensic AI

Our tool utilizes a "Chain of Evidence" logic to provide:

1. **Deep Analysis:** Cross-referencing statements from all stakeholders to find inconsistencies.
2. **Perpetrator Profiling:** Instant classification of "Internal Employee" vs. "External Fraudster."
3. **Department Mapping:** Specifically identifies the department and the internal "gate" (process) that was bypassed.

Value Proposition

- **Speed to Resolution:** Reduces the forensic timeline from 14 days to under 2 minutes.
- **Cost Reduction:** Minimizes the need for expensive third-party forensic consultants.
- **Objective Evidence:** Provides a fact-based report that can be used as a basis for legal action or process hardening.

Data Security & Privacy

The tool is designed for high-security environments. It analyses the context provided in incident reports without requiring direct integration into core banking databases unless desired, ensuring total control over PII (Personally Identifiable Information).