CUSTOMER SUCCESS STORY

Orchestrated Case Management

Process Became the First Line of Defence Against Financial Crime for a National Intelligence Agency

Industry: **Government & Financial Intelligence**
Platform: **NewgenONE Case Management**

Highlights

- Data Management of 40k-60k Reporting Entities
- Entity Network Visualization & Mapping
- AI/ML-driven Red Flag Detection
- Rule-based Case Dissemination
- Real-time Case Linking & Scoring
- Multi-agency Intelligence Integration with 140+ LEAs

THE CLIENT

A National Guardian Against Financial Crime

Our customer is a high-level governmental and national agency, tasked with one of the most consequential mandates in financial security, including monitoring, gathering, analyzing, and reporting intelligence on suspicious financial transactions and associated crimes with law enforcement agencies across the country.

Operating at the intersection of finance, law enforcement, and national security, the agency received transaction reports from banks, financial institutions, and a broad network of reporting entities. Its decisions, which cases to investigate, which to escalate, which patterns to flag, had direct consequences for the integrity of the national financial system and the prosecution of financial crime. Yet, despite the gravity of its mission, the agency operated with tools and processes ill-matched to the scale, complexity, and speed of modern financial crime. Manual workflows, fragmented systems, and the absence of intelligent orchestration meant that analysts had to spend more time managing processes than detecting threats.

The Challenge:
Where the Agency's Operations Broke Down

Financial crime was inherently networked, fast-moving, and deliberately deceptive. Detecting it required precision, speed, and the ability to see connections across thousands of cases simultaneously. The agency's existing environment could deliver none of these at the scale demanded.

#01 Complexity in Monitoring and Reporting Transactions

Transactions arrived from banks, financial institutions, and reporting entities in multiple formats and channels. Analysts had no unified view, making it a challenging task to spot patterns, correlate data, or escalate cases promptly. Volume compounded the problem, and scale was only growing.

#02 Inaccurate and Inconsistent Case Linkages

Without intelligent cross-referencing, related cases remained siloed. Investigators manually searched for connections, which was a slow, error-prone process that left suspicious networks invisible across case boundaries.

#03 Absence of a Systematic Case Analysis Methodology

There was no structured framework to assess risk, prioritize cases, or generate consistent intelligence summaries. Every analyst followed their own approach, leading to uneven outcomes, missed red flags, and an inability to build institutional intelligence over time.

#04 Inefficient Communication Between Stakeholders and Law Enforcement

Information exchange between the agency, law enforcement agencies, and reporting entities depended on manual emails and phone calls. Delays were common, timelines were unpredictable, and audit trails were fragile, resulting creating compliance exposure at every handoff.

#05 Lack of Rule-based Case Dissemination

Cases were routed and shared based on individual judgment rather than defined rules, creating bottlenecks, inequitable workloads, and gaps in how, and whether, intelligence reached the enforcement bodies that needed it most.

At the core of all five challenges was a single structural problem, the absence of an intelligent, unified orchestration layer that could connect data, automate analysis, and govern the entire case lifecycle without human bottlenecks at every decision point.

The Decision

The agency recognized early that process improvement alone would not close the gap. Digitizing the existing manual workflow would only automate its limitations. What was needed was a completely different operating model, one where AI was not a feature layered onto the process, but the engine that drove it. The transformation priorities were clearly defined, including:

- Replace manual case analysis with AI-driven risk scoring and real-time pattern detection
- Automate the identification and linking of related cases across the entire case database
- Establish governed, rule-based workflows for case routing, assignment, and dissemination
- Enable real-time, structured communication with law enforcement and regulatory bodies
- Create a unified, auditable case management environment. from intake through to closure

To achieve this, the agency partnered with Newgen and deployed an intelligently orchestrated case management solution, built on NewgenONE platform. The platform orchestrates intelligent enterprises while combining native process automation, content services, and communication management into a single orchestration layer. The result was not a system that supports investigations. It was a system that drives them.

THE SOLUTION

AI Woven Across Every Stage of the Case Lifecycle

Each feeds the next, forming a closed-loop system where every case is continuously enriched, scored, linked, and acted upon, without human intervention at routine decision points.

INTELLIGENCE LAYER 01

AI-driven Case Intake and Data Extraction

Every case began with data and data quality determined everything downstream. The platform deployed AI-driven extraction to pull structured information from identity documents, passports, PAN cards, corporate filings, submitted during entity registration. Rather than relying on analysts to manually key in details, AI read, validated, and ingested the data automatically.
The extraction layer handled varied document formats, inconsistent image quality, and multi-lingual inputs without degrading accuracy. From the moment an entity registered or a case was initiated via the online portal, AI was already at work, converting raw inputs into governed, searchable intelligence records.

- Automated extraction from passports, PAN cards, and corporate identity documents at point of registration
- AI validated entity data before it entered the system, eliminating manual keying errors and duplicate records
- Online portal integration ensured every case entered a governed intelligence pipeline from day one
- Unstructured inputs converted to structured, searchable records with no analyst intervention required

INTELLIGENCE LAYER 02

ML-driven Red Flag Detection and Case Linking

Once a case entered the system, the AI/ML engine activated a continuous layer of pattern intelligence. Rather than waiting for an analyst to flag a concern, the engine proactively scanned every case against historical data, rule-based indicators, and cross-case relationship graphs.
If a reporting entity had appeared in a previous suspicious transaction, even under a different case number, institution, or jurisdiction, the system surfaced that connection instantly.
Red flag indicators fired automatically when a case matched predefined risk criteria. Similar cases were linked, giving investigators a network view that no manual search could replicate at scale.

- Rule engine evaluated every incoming case against a library of configurable red flag indicators
- ML models surfaced patterns from historical data and generated instant, evidence-based case summaries
- Similar cases linked automatically, building entity relationship networks in real time across the full database
- AI-generated suggestions directed analysts toward the highest-risk cases first, before investigation began

INTELLIGENCE LAYER 03

Analytics Platform and Entity Relationship Visualization

Networks of entities, individuals, shell companies, intermediaries, operated across multiple transactions to obscure money flows. Detecting these networks required a visual, relational view that static case files could not provide.

NewgenONE integrated with a dedicated analytics platform transformed raw case data into dynamic network diagrams. Analysts could trace connections between entities across cases, jurisdictions, and transaction types, identifying rings, clusters, and anomalies that would remain invisible inside individual case records. The network view became a live intelligence asset, updated automatically as new cases entered the system.

- Entity relationship diagrams built automatically from cross-case data, no analyst construction required
- Visual network maps exposed shell structures, intermediary chains, and suspicious clusters at a glance
- Analysts navigated complex financial crime networks through a single, integrated analytics interface
- Network intelligence fed back into each case record, continuously enriching every future investigation

INTELLIGENCE LAYER 04

Rule-based Case Routing, Dissemination, and Law Enforcement Agencies (LEA) Integration

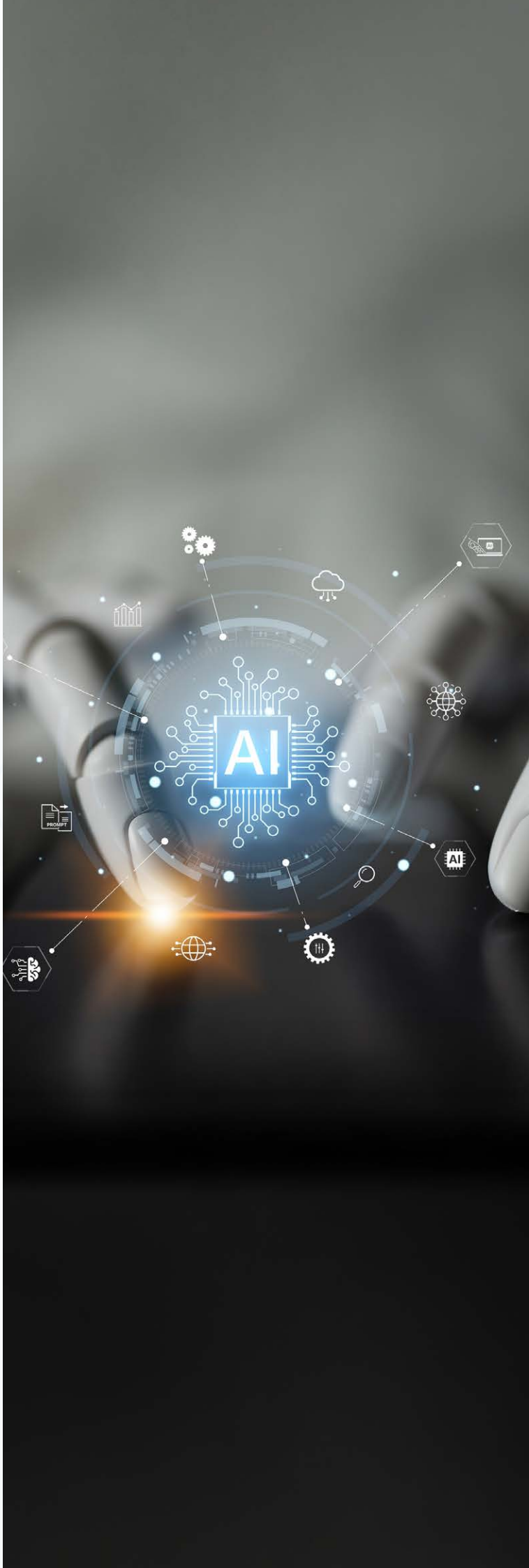
Intelligence was only as valuable as the speed at which it reached the right hands. Before this transformation, case dissemination to law enforcement agencies was a manual, judgment-driven process, unpredictable, inconsistent, and impossible to audit comprehensively. Post the implementation, routing was governed by configurable business rules, ensuring every case reached the appropriate LEA, regulatory body, or internal team based on type, risk level, jurisdiction, and defined criteria, automatically.
Bi-directional integration with intelligence and regulatory agencies enabled seamless data sharing and ingestion. Requests from LEAs triggered structured response workflows. Counterfeit currency reports, cross-border transaction filings, and reporting entity registrations each followed dedicated, governed pathways. Case dissemination was no longer a bottleneck, it was an automated, auditable event.

- Business rule engine determined case routing and dissemination without manual intervention at any step
- Bi-directional integration with LEAs enabled real-time request-response workflows with full traceability
- Dedicated workflows handled counterfeit currency, cross-border transactions, and entity registrations
- Every dissemination event logged automatically-creating a complete, searchable, compliant intelligence trail

UNIFIED MULTI-AGENCY INTELLIGENCE ECOSYSTEM

A Unified Intelligence Network Operating at National Scale

The agency sat at the nerve center of a nationwide financial intelligence ecosystem, receiving and managing data from 40k–60k reporting entities, coordinating with dozens of regulatory bodies, and exchanging intelligence with over 140 law enforcement agencies across central and state jurisdictions. At this scale, the platform's core job was not just to connect these participants. It was to keep them in continuous, collaborative motion. The integration with LEAs was live and bi-directional. When a case was escalated, the platform packaged and disseminated the relevant intelligence to the right agency. When LEAs responded with investigation requests, updates, or findings, that data flowed back into the system through structured workflows, updating case records in real time. Every stakeholder stayed synchronized. Every exchange was logged, timestamped, and traceable. What made this work at national scale was the platform's agility; the ability to handle high volumes of incoming and outgoing data without breaking stride, such as ingesting reports, enriching cases, routing intelligence, and processing responses simultaneously, across hundreds of active cases and dozens of agencies at any given moment. The collaborative network did not slow down as it scaled, it got sharper.



Reporting Ecosystem

40k–60k reporting entities

- Banks and financial institutions
- NBFCs and cooperative banks
- Housing finance companies
- Financial intermediaries and market participants
- Chit fund organizations and regulated financial entities

Regulatory & Government Authorities

- Banking and financial regulators
- Securities and market regulatory authorities
- Insurance and pension authorities
- Taxation and revenue departments
- Customs and cross-border transaction monitoring authorities
- Financial compliance and supervisory bodies

Law Enforcement & Investigation Agencies

140+ Law Enforcement Agencies (LEAs) across central and state jurisdictions

- National investigation and intelligence organizations
- Financial crime and anti-money laundering enforcement agencies
- Economic offences and fraud investigation
- Revenue intelligence and enforcement authorities
- Cybercrime investigation units
- Cross-border transaction and illicit trade monitoring agencies
- State-level law enforcement and prosecution departments
- Specialized financial investigation and compliance enforcement teams

International Intelligence Collaboration

- Global Financial Intelligence Unit (FIU) networks
- FATF-aligned intelligence and compliance ecosystems
- International law enforcement coordination agencies
- Cross-border intelligence sharing frameworks
- Bilateral and multi-lateral financial intelligence partnerships

THE PIPELINE

How a Case Moved Through the System-End-to-end

What the agency's analysts experience today is a case environment where each stage hands off to the next without waiting for someone to pull a file, re-enter data, or manually trigger an action. Here is what happens, and what AI does, at every touchpoint:

Stage	What the System Does	AI's Role
Case Initiation	Transaction reports arrive via the online portal from banks, financial institutions, and reporting entities.	AI validates entity identity data at registration; flags duplicate or inconsistent submissions before they enter the case record.
Data Extraction	Identity documents, passports, PAN cards, corporate filings, are processed and structured into governed records.	AI reads and extracts key fields with high accuracy regardless of document format, language, or image quality. No manual keying.
Risk Scoring & Red Flag Detection	Each case is evaluated against the agency's risk criteria and rule library before any analyst sees it.	The ML engine fires red flag indicators, assigns risk scores, and surfaces historical matches automatically, in real time.
Case Linking & Network Mapping	Related cases, entities, and transactions are cross-referenced across the full case database.	AI links similar cases instantly. The analytics platform renders entity relationship and network diagrams without analyst input.
Case Summary Generation	Analysts receive a pre-built intelligence summary drawn from case data and historical records.	The ML model synthesises evidence and generates AI-driven suggestions that guide the investigation, before it begins.
Routing & Dissemination	Cases are assigned and shared with internal teams, LEAs, and regulatory agencies.	The rule engine governs every routing decision. No manual judgment required. Every action logged in a complete audit trail.
LEA Request Response	Law enforcement agencies submit requests; the agency compiles and delivers structured intelligence packages.	Automated workflows manage request intake, data compilation, and response delivery from end to end.

THE IMPACT

What Changed for the Teams Who Use It

The transformation served 2 communities whose daily work depends on intelligence in different ways and improved the experience of both.

For Intelligence Analysts	For Operations & Compliance Teams
Cases arrive pre-scored, pre-summarized, and pre-linked, analysts assess, they no longer assemble	Case routing is governed by rules, no manual assignment, no inconsistent workload distribution
Red flag indicators fire automatically, directing attention to the highest-risk cases first	LEA requests are managed through structured workflows, no email chains, no missed response timelines
Network diagrams reveal entity relationships across cases and jurisdictions in seconds, not hours	Every action is logged in the centralized repository, audit preparation requires no reconstruction
Historical pattern matches surface before an analyst types a single search query	Compliance reporting draws on governed, consistent data, not individual analyst recollection

OUTCOMES
Where the Transformation was Felt

Outcome Area	Result
Case Workflow Automation	End-to-end automation of case intake, routing, analysis, and dissemination, eliminating manual handoffs across the entire lifecycle.
Red Flag Accuracy	The rule engine and ML models surface risk indicators consistently, replacing analyst guesswork with governed, evidence-based alerts every time.
Case Linking Speed	AI links related cases and entities in real time, connections that previously required hours of manual cross-referencing now surface instantly.
Entity Network Visibility	The analytics platform renders relationship and network diagrams automatically, giving investigators a visual command of complex financial crime structures.
LEA Communication	Structured request-response workflows replaced ad hoc communication, every interaction logged, traceable, and compliant.
Case Dissemination	Rule-based routing ensures cases reach the right agencies without delay, bottleneck, or manual routing decisions.
Process Transparency	Every action, extraction, scoring, routing, dissemination, is logged in the centralized repository with a full and searchable audit trail.
Regulatory Compliance	Standardised, rule-governed case handling ensures consistent compliance with reporting requirements across all transaction types.

BENEFITS ACHIEVED

What the Agency Gained

The deployed case management solution transformed a fragmented, analyst-dependent operation into a governed, intelligence-driven function. Cases no longer moved at the speed of human availability, they moved at the speed of the system. Every step, from intake to dissemination, was automated, auditable, and consistent.

- Optimized case management process, from intake to closure without manual bottlenecks
- Reduced operational inefficiencies across the full case workflow
- Improved investigative agility, analysts focused on decisions, not data management
- Robust, real-time integration across the agency's ecosystem of systems and partners
- Comprehensive reporting and monitoring capabilities across all case types
- Enhanced process transparency and control, every action logged and searchable
- AI-informed decision making, risk scores, summaries, and suggestions at the point of need
- Better regulatory compliance, standardized, rule-governed handling across all transaction types

Summing Up

Financial crime does not wait. Suspicious transactions are structured to be invisible, networks are designed to be opaque, and patterns are deliberately fragmented across institutions, geographies, and time. Detecting them requires a system that can outpace human bandwidth, one that sees everything, connects everything, and acts without delay.

With the intelligently orchestrated case management solution, the agency built exactly that. AI no longer sits at the edge of the investigation process, it sits at the center. It reads documents, scores risk, links cases, maps networks, generates summaries, routes intelligence, and logs every action for compliance. Analysts who once spent their time managing information now spend it acting on it.

The transformation is not just operational. It is structural. The agency now has a case management backbone built for the complexity of modern financial crime, governed by intelligence, driven by data, and designed to scale as both threat volumes and regulatory demands grow.

About Newgen

Newgen Software Orchestrates Intelligent Enterprises at scale. The NewgenONE Platform unifies content, processes, and communications into an orchestration layer where intelligence is embedded into how enterprises operate, with trust, governance, and control built in. Enterprises move beyond fragmented initiatives to continuously adaptive, production-ready operations. Decisions, workflows, and experiences evolve in real time, shaped by context, data, and embedded AI. Trusted by leading organizations worldwide, Newgen defines how modern enterprises operate, intelligently and at scale.

For Sales Query

AMERICAS: +1 (202) 800 77 83

CANADA: +1 (202) 800 77 83

AUSTRALIA: +61 290 537174

INDIA: +91 11 407 73769

APAC: +65 3157 6189

MEA: +971 600 521 468, +27 11 461 6497

EUROPE: +44 (0) 2036 514805

info@newgensoft.com

www.newgensoft.com

newgen