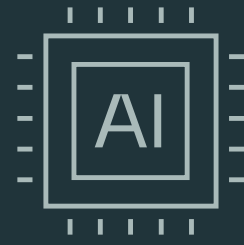


Suspicious transaction response management with Agentic AI



Banking

Business challenge and opportunity

Banks frequently receive high volumes of data and financial action requests from country cyber-crime agencies including platforms like the Indian Cyber Crime Coordination Centre (I4C) or the U.S. FBI Internet Crime Complaint Center (IC3). These requests demand swift action on specific accounts, often accompanied by PDF acknowledgments containing complaint details and suspicious transaction data. The current processes rely heavily on manual intervention by Financial Risk Management (FRM) teams.

Analysts must manually extract customer information, transaction details, and complaint specifics to execute actions like account blocking or lien marking. This multidimensional data demand creates significant operational bottlenecks. For banks handling thousands of requests, manual processing introduces risks of delay, human error, and compliance lapses.

Automating this workflow with an AI agent presents a critical opportunity. It allows banks to respond to agencies rapidly, accurately and more cost-effectively, supporting regulatory compliance while freeing FRM teams from repetitive data extraction tasks to focus on higher-level risk assessments, like complex fraud investigations.

Technical challenges

Banks aiming to help cyber-crime agencies have common technical hurdles to cross to streamline the process with Agentic AI:

- 1. Unstructured inbound data formats**
Incoming requests arrive as PDF acknowledgment forms with dense, non-standardized content, making the data inherently difficult for systems to interpret.
- 2. Inability of legacy systems to process PDFs**
Core banking and legacy platforms cannot natively read or extract data from unstructured PDF documents, preventing automated workflow initiation.
- 3. Data locked deep within core banking systems**
Required response data such as Customer Information Files (CIF) details, transaction summaries, and sub-categorized analytics reside across multiple layers of core systems, making it difficult to extract important data easily.
- 4. Manual, error-prone data bridging**
Manually bridging the gap between unstructured PDF inputs and structured core banking data is error-prone.
- 5. Lack of an intelligent layer**
Without a smart layer to parse documents and orchestrate backend queries, banks struggle to scale response capabilities and keep pace with growing regulatory demands.

Our solution

Using the **Kyndryl Agentic AI Framework**, Kyndryl can help banks with:

- **End-to-end automation of suspicious transaction responses**
Managing suspicious transaction responses is complex and labor-intensive when handled manually. Automating the full lifecycle reduces reliance on manual effort and streamlines how responses are created, reviewed and submitted.
- **Reduced manual effort for financial risk teams**
FRM teams spend significant time handling repetitive, administrative tasks instead of higher-value work. The intelligent agent interfaces directly with the FRM workflow, minimizing manual steps and easing operational burden on the team.
- **Accurate extraction of critical data from PDFs**
Acknowledgment PDFs contain essential information but are difficult to process accurately by hand. Automatic extraction of account numbers and suspicious transaction unique reference identifiers eliminates manual data entry and reduces transcription errors.
- **Validation for confidence and control**
Banks need confidence in the accuracy of extracted data, especially for regulatory responses. Presenting extracted data on a dashboard for rapid user confirmation balances automation with oversight.
- **Automated retrieval of required data from core systems**
Response data such as CIF details and transaction summaries resides deep within core banking systems. The AI agent automatically pulls all required data elements based on extracted inputs, removing the need for manual system navigation.
- **Consistent, standardized regulatory response output**
Regulatory agencies expect responses to follow a clear and consistent format. Automatically generating a standardized response PDF supports consistent, readily available submissions.
- **Readiness of underlying data architecture for AI integration**
AI-driven automation depends on a well-prepared data foundation. Kyndryl Consult can help banks prepare their data architecture to support deep integration with core systems.
- **Secure and auditable handling of sensitive financial data**
Suspicious transaction data is highly sensitive and subject to strict governance requirements. A secure, scalable framework enables banks to handle data in accordance with their governance and auditability requirements.



Benefits you could achieve

Automating the suspicious transactions workflow with an AI agent can allow banks to respond to agencies more quickly, with the potential to:

- **Eliminate manual extraction:** Remove the need for analysts to manually read and type data from PDF acknowledgments, significantly reducing processing time.
- **Enhance data accuracy:** Reinforce consistency in capturing Unique Transaction References (UTRs) and account details, mitigating the risk of incorrect account freezes or missed transactions.
- **Accelerate regulatory compliance:** Significantly shorten the turnaround time for the bank to respond to regulatory requests, helping the bank meet their regulatory requirements.
- **Standardize response quality:** Generate uniform, comprehensive response documents that automatically include all required transaction analytics and summaries.
- **Optimize workforce productivity:** Shift your FRM team's focus from administrative data gathering to strategic risk analysis and complex fraud investigations.

One Kyndryl customer realized more than 50% reduction in STR processing time through the integration of Agentic AI.¹



Why Kyndryl?

With decades of mission-critical operations experience, we bring deep expertise in designing, building, and managing AI across complex IT estates.

The **Kyndryl Agentic AI Framework** brings together the right governance and security controls and human oversight to enable businesses to move beyond isolated pilots to integrated, intelligent systems. It combines secure, scalable agent orchestration with real-time observability and governance, powered by **Kyndryl Bridge**.

Through **Kyndryl Consult**, we align AI strategy with business outcomes. **Kyndryl Vital** provides proven user-centered design and rapid prototyping. And our trusted **delivery experts** support frictionless integration and help with reskilling and upskilling to build the foundation for success at scale.

We apply a forward engineering approach—using insights from existing systems to design and deploy future-ready AI agents and architectures that are adaptive, resilient, and scalable. Our method is grounded in open ecosystems, data sovereignty, and transparent decision-making.

And with a carefully selected **alliance ecosystems**—across cloud, data, and AI—we bring the right partners and technologies together to design fit for purpose solutions and orchestrate AI at scale without disrupting the business.

With Kyndryl, AI becomes a core capability—not just a tool—driving productivity, innovation, and growth.

Accelerate your journey to AI-native

Our AI Benchmark Assessment provides a maturity snapshot and personalized roadmap for accelerating the value of AI in your organization.

Take the assessment →

What's your enterprise vision for AI?

Let's co-create it together.

Talk to an expert →

kyndryl.

© Copyright Kyndryl, Inc. July 2026

Kyndryl is a trademark or registered trademark of Kyndryl Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl Inc. or other companies. This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

1. Outcomes described in this use case are those of a single customer. Individual customer results will vary. Kyndryl makes no representation or warranty that any other entity will experience the same or similar results.