TRANSFORMING SANCTIONS COMPLIANCE WITH AI

October 31, 2025 Frank Morisano

Artificial Intelligence and Financial Crime Prevention

Sanctions compliance is foundational to financial crime prevention, yet traditional screening approaches such as name-based matching against public watchlists, issued by the U.S. Treasury's Office of Foreign Assets Control (OFAC), that use static logic, or fuzzy matching algorithms are no longer sufficient. These outmoded approaches generate excessive false positives, swamp investigation teams to perform manual reviews, and ignore sophisticated evasion techniques that leverage intermediaries, shell entities, and layered ownership structures to identify money laundering. The 2020 Bank Policy Institute report[1] underscores this issue, it states that "name-based screening frequently produces no true positives while consuming disproportionate compliance resources".

Financial institutions must modernize sanctions compliance. Artificial Intelligence (AI) enables real-time analysis of vast, heterogeneous datasets to detect behavioral anomalies and transaction patterns that name-matching currently cannot reveal to financial institutions. These advanced technologies enhance senior management decision-making with objective, data-driven alerts while improving consistency and the auditability of the financial crime programs. Generative AI adds further value by analyzing unstructured and relevant data, such as news, filings, and social media to provide context and reduce false positives. The integration of sanctions screening, Anti-Money Laundering (AML), and Know Your Customer (KYC) data allows financial institutions to dismantle internal silos and build comprehensive risk profiles of the customers.

Success with AI systems begins with the financial institution implementing rigorous data governance programs. Even the most advanced AML models fail to perform due to stale, incomplete, or poorly linked customer data. Financial institutions must enforce continuous data quality, data provenance, and data source coverage. Equally critical is early, sustained engagement with the regulators to align innovation with supervisory expectations. Financial institutions that integrate frameworks and programs with advanced AI-driven transaction monitoring and sanction screening tools, implement robust data governance frameworks,

[1] Bradfield, Angelena (2020). Reforming the U.S. Sanctions Regulatory Regime: How a Smarter, Risk-Based Approach Can Make Sanctions More Effective. https://bpi.com/reforming-the-u-s-sanctions-regulatory-regime-how-a-smarter-risk-based-approach-can-make-sanctions-more-effective/

and maintain proactive regulatory dialogue will be better prepared to address the evolving sanctions compliance situation.

RETHINKING SANCTIONS COMPLIANCE

Traditional name-based screening and static watchlists remain necessary components of sanctions compliance but are no longer sufficient on their own. Surface-level text matching is easy to deploy yet fundamentally limited as it cannot reliably resolve complex ownership structures, trace intermediary channels, or pierce deliberate obfuscation designed by money launderers to defeat list-based controls. As a result, legacy systems generate disproportionate false positives that swell alert queues, consume scarce investigative capacity, and may obscure genuine threats.

A primary failure of traditional screening models is their fleeting effectiveness after public designation and appearance on sanctions lists. Entities and networks adapt quickly once listed, causing name hits to spike briefly and then fade, while true positives remain scarce. Empirical analyses have shown that conventional name-based approaches frequently yield almost no sustained true matches, leaving compliance teams overwhelmed with low-value alerts and diverting attention from the behavioral factors that matter most in financial crime prevention.

Implementing AI systems reframe sanctions screening into an intelligence-driven, risk-first capability rather than an after-the-fact checkbox exercise. At the core of this paradigm shift is persistent entity resolution and graph analytics that link individuals, legal entities, accounts, addresses, and transactional flows. Identity graphs reveal hidden ownership, control relationships, and intermediary pathways that static lists cannot; these tools enable investigators to follow the money and expose layered corporate structures used for sanctions evasion.

Complementing identity resolution, behavioral and anomaly detection models powered by AI captures deviations from established baselines (unusual routing, velocity, concentration, or layering) that indicate intent to evade sanctions. These models prioritize signals over strings, surfacing high-risk activity even when names do not appear on any list. Integrating unstructured intelligence from news, filings, court records, social media through natural language processing (NLP) and generative AI further enriches context, uncovers aliases and temporal indicators, and reduces false positives by adding corroborative evidence to alerts.

Robust data governance must underpin these technical advancements. Financial institutions require centralized and authoritative master data management with provenance, versioning, and continuous reconciliation to ensure the models use accurate inputs; human-in-the-loop feedback mechanisms use investigator outcomes to retrain the AI models and mitigate drift; and explainability and independent validation preserve auditability and regulator confidence. Without disciplined data practices, even the most sophisticated analytics will underperform.

Operational integration is equally important. Consolidating sanctions screening, AML, KYC, transaction monitoring, and trade surveillance produces unified risk profiles and prevents siloed alerting. Risk-based orchestration routes high-priority cases to specialist compliance teams, automates repeatable investigative steps, and codifies playbooks for consistent escalation and remediation. A phased implementation is best practice for identifying gaps, piloting graph and behavioral solutions, scaling data management and model governance, and maintaining continuous monitoring and regulatory engagement to deliver measurable improvements.

As financial institutions progress from static list-matching to layered, intelligence-led screening, they can reduce false positives, detect sophisticated sanctions evasion techniques earlier, and make faster, more defensible compliance decisions. This is the pragmatic pathway to turning sanctions screening from reactive control into proactive risk orchestration.

AI-POWERED RISK DETECTION

AI is reshaping the field of sanctions compliance and offering financial institutions a powerful toolkit to detect risk with greater precision and speed. Traditional screening systems that are reliant on static rules and fuzzy matching struggle to keep pace with the complexity and velocity of global transactions. In contrast, AI systems, particularly those powered by machine learning and large language models (LLMs), are proving capable of analyzing vast datasets in real time, identifying subtle patterns and anomalies that human analysts might overlook.

A recent study by the Federal Reserve Board[2] highlighted the impact of LLMs in sanctions screening, showing a 92% reduction in false positives and an 11% increase in true matches compared to the most advanced fuzzy matching systems. These models not only improve screening accuracy but also enhance operational efficiency by reducing investigative backlogs and enabling faster triage of high-risk cases.

Beyond transactional analysis, AI systems can enrich contextual understanding. Generative AI models process unstructured data such as news articles, regulatory filings, and social media posts to uncover hidden affiliations, reputational risks, and geopolitical exposure. This capability allows financial institutions to move beyond list-based screening and toward dynamic entity profiling, where risk assessments address both structured and unstructured domains.

Sanctions compliance teams also benefit from AI's research and synthesis capabilities. By automating the aggregation of regulatory guidance and precedent, AI helps standardize interpretations across jurisdictions, reducing ambiguity and improving the consistency of internal

[2] Allen, Jeffrey S., and Max S. S. Hatfield (2025). Can LLMs Improve Sanctions Screening in the Financial System? Evidence from a Fuzzy Matching Assessment, Finance and Economics Discussion Series 2025-092. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.092.

policy application. Moreover, AI-generated narratives and audit trails support defensible decision-making, aligning with evolving supervisory expectations around explainability and governance.

The fusion of predictive and generative AI marks a significant leap forward for financial crime modeling. Predictive models flag behavioral anomalies and transactional irregularities, while generative systems provide the narrative and contextual depth needed to understand and act on those alerts. Together, they enable financial institutions to reduce false positives, capture complex evasion tactics, and deliver more robust, regulator-ready compliance outcomes.

CONVERGENCE OF SANCTIONS, AML, AND KYC

The traditional silo separation of sanctions screening, AML, and KYC functions is no longer tenable to stop money laundering. Financial crimes increasingly straddle multiple domains while sanctioned entities use complex customer relationships to launder proceeds, layered corporate structures hide beneficial ownership, and transactional anomalies signal both sanctions evasion and money laundering. Operating these controls in a silo manner creates detection blind spots, inflates false positives, and wastes investigator bandwidth. Financial institutions need to integrate the sanctions screening, AML, and KYC processes to build resilient, efficient, and forward-looking compliance programs.

An integrated approach begins with a single, persistent identity data layer that consolidates customer, counterparty, and third-party information into a centralized master record. Entity resolution and persistent identity graphs reconcile aliases, subsidiaries, addresses, and accounts to reveal hidden relationships and control links. When sanctions screening consumes the same cleaned, reconciled identity data used by AML and KYC, alerts are more-comprehensive, more-contextual, and less likely to be duplicative.

Behavioral analytics provides the second critical layer. Rather than relying solely on static list matches, machine learning models observe baseline behaviors across payments, trade flows, account openings, and onboarding documentation. Deviations such as sudden routing changes, structuring, or sudden relationships with higher-risk jurisdictions create alerts that cut across sanctions and AML typologies. Integrating these insights into a consolidated risk score enables prioritized workflows that focus human attention where it is required.

Unstructured analytics acts as a force multiplier. Natural language processing and generative AI ingest adverse media, regulatory notices, legal filings, shipping manifests, and social media to extract aliases, contextual events, and temporal risk indicators. When fused with structured KYC and transaction data, this analysis enhances the comprehensiveness of alert data and supplies corroborating evidence that reduces false positives and speeds investigations.

Data governance and data provenance are foundational to integration. Convergence demands rigorous master data management, standardized taxonomies for risk attributes, and clear lineage

for every data element. Continuous reconciliation, data provenance tracking, and version control ensure that models and analysts work from the same, auditable data source of truth. Model data governance, model transparency, and back-testing are non-negotiable; they provide defensibility in supervisory reviews and internal audits.

Operational redesign completes the transformation to the new paradigm. Converged programs require integrated case management, shared triage thresholds, and cross-functional playbooks that align sanctions, AML, and KYC response actions. Complex network cases that are identified are routed to multidisciplinary risk and compliance teams while at the same time automating routine remediations. Newly designed feedback loops allow investigative outcomes to directly retrain models and update identity graphs as well as sharpen detection over time.

The business case for convergence is compelling resulting in fewer false positives, faster time-to-resolution, earlier detection of sophisticated evasion, and reduced compliance cost through automation and the elimination of duplicate alerts. Equally important is regulatory alignment; supervisors expect holistic programs that address enterprise-wide risk rather than fragmented solutions. Early, transparent engagement with regulators regarding data lineage, model controls, and governance accelerates adoption, decision-making, and builds trust.

Convergence is a technical and cultural journey for every financial institution. It requires investment in data architecture, advanced analytics, integrated modeling, and change management to break legacy compliance silos. Financial institutions that commit to a unified identity backbone, behavioral AI systems, unstructured intelligence integration, and disciplined governance will turn sanctions compliance from a defensive cost center into a strategic capability that proactively mitigates multi-dimensional financial crime risks.

THE TIME IS NOW

Financial institutions must move decisively to understand, evaluate, and adopt the right financial crime prevention solutions. Familiarity with emerging technologies, particularly those powered by AI, is no longer optional; it is essential for maintaining regulatory alignment, operational resilience, and a strategic advantage in the industry. The adoption curve can be steep, but proactive engagement and internal readiness will significantly ease the transition.

Regulators, too, are navigating a rapidly evolving technology landscape. Their challenge lies not only in understanding the technical underpinnings of AI systems, but also in assessing their implications for risk management, governance, and supervisory oversight. For financial institutions seeking to deploy advanced technologies, early and sustained engagement with their regulators is critical. Transparent dialogue, shared learning, and collaborative testing can help build regulatory confidence, reduce friction, and foster a more adaptive and innovative-friendly compliance environment. Overall, this approach benefits the entire ecosystem. When regulators

are comfortable with the design, controls, and explainability of AI systems, they are more likely to support their use at scale paving the way for industry-wide modernization of sanctions compliance.

The integration of AI technologies while enhancing data quality, and the dismantling silos between compliance, risk, and technology functions, allow financial institutions to dramatically improve their ability to detect sanctions violations, respond to emerging money laundering threats, and mitigate reputational and regulatory exposure. Now is the time for financial institutions to lead with innovation, invest in transformation, and shape a more intelligent, agile, and accountable compliance paradigm.

The future of sanctions compliance is not on the horizon; it has arrived!

#Sanctions #Compliance #Risk #KYC #AML #OFAC #Regulation #ArtificalIntelligence #AI #NLP #LLM #data