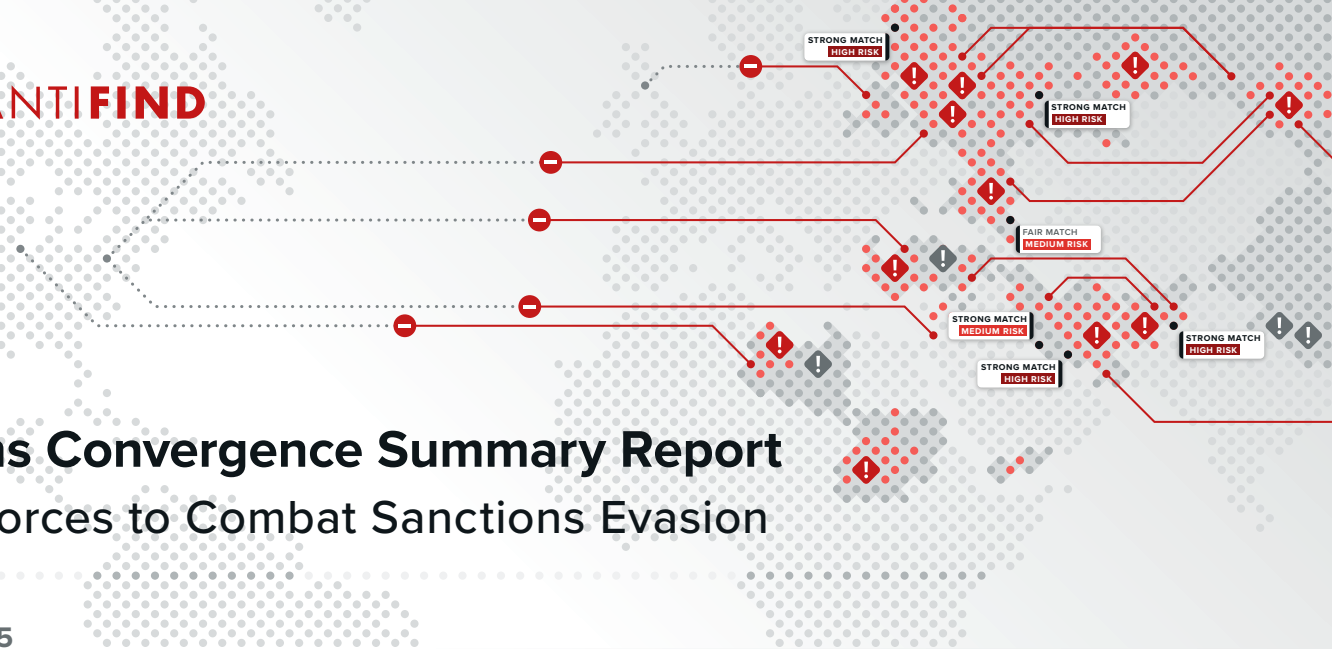
QUANTIFIND



Sanctions Convergence Summary Report

Uniting Forces to Combat Sanctions Evasion

JUNE 24, 2025

Event Overview

Sanctions enforcement is entering a new era. As geopolitical tensions rise and evasion tactics grow increasingly sophisticated, financial institutions must rethink how they detect and respond to sanctions-related risk. At our recent **Sanctions Convergence** event: **Uniting Forces to Combat Sanctions Evasion**, hosted by **Quantifind** and **Protiviti**, experts from across financial services, government, and technology came together to share perspectives and chart a more coordinated path forward.

We want to extend our sincere thanks to all participants. Your thoughtful contributions during the panel and roundtable discussions helped surface meaningful insights, practical strategies, and emerging opportunities to strengthen sanctions compliance.

This report summarizes the event's key takeaways: from detection gaps and regulatory expectations to the role of AI and cross-industry collaboration. We hope it supports continued dialogue and innovation across the sanctions compliance community.

PANEL SUMMARY

Sanctions Evasion, Detection, and the Role of AI

This expert panel explored the converging threats, expectations, and technologies shaping modern sanctions enforcement. Speakers shared real-world examples, explored evolving adversary tactics, and discussed the promise and limits of AI in enhancing compliance efforts.

Key Themes and Insights

Evolving Adversarial Tactics

- Criminals are employing multi-layered evasion schemes, including falsified shipping documents, cryptocurrency, third-party intermediaries, and shell networks.
- Trade-based evasion (e.g., Iranian oil transfers) and bundling of tactics complicate detection.
- Professional enablers such as brokers, accountants, lawyers, and real estate agents are increasingly used as “referral points” to obscure ownership and evade detection. These actors often operate one step removed from sanctioned entities, making conventional screening ineffective.

Detection and Technology

- Siloed teams, human error, and lack of feedback loops remain weak points.
- Data quality issues often reflect deeper process or governance breakdowns.
- There’s a growing consensus on the need to converge AML and sanctions frameworks.
- Many institutions face manual bottlenecks in trade finance, where paper-based letters of credit and bills of lading delay alert investigation and elevate risk. The time-sensitive nature of these documents often forces banks to prioritize speed over deeper diligence.

Operational and Strategic Recommendations

- Integrate sanctions, AML, export control, and tariff evasion workflows.
- Develop models that anticipate emerging risks, not just react to existing lists.
- Tailor compliance programs to jurisdictional differences and evolving enforcement priorities.
- Prepare for cartels newly designated as terrorist entities, which will require major updates to KYC frameworks, onboarding workflows, and external data sourcing strategies, especially in Latin American regions.

©2025 Quantifind, Inc.

Regulatory Expectations and Global Coordination

- Regulators are focused on China, Iran, and cartel-related activity.
- Financial institutions are expected to adopt new standards (like ISO 20022) and leverage external data sources.
- Coordination surged during the Ukraine conflict but may fragment due to shifting political tides.
- With the FFIEC removing reputational risk from examiner portfolios, banks are left to independently assess whether to onboard or retain customers who pose reputational concerns—regardless of legal permissibility. This increases internal scrutiny and raises the stakes for compliance teams.

Artificial Intelligence: Promise and Pitfalls

- AI is gaining traction, especially in triage and pattern recognition.
- Success depends on clean data, explainable models, and strong governance.
- Regulators are increasingly engaged and expect human oversight, not automation alone.
- Regulators themselves are adopting AI tools, raising the bar for transparency and sophistication from financial institutions. This creates asymmetric pressure, as banks are evaluated by increasingly intelligent systems while still grappling with legacy tools.
- AI is particularly helpful for triaging multilingual adverse media and connecting complex ownership networks, but its role must remain assistive, not determinative.

ROUNDTABLE SUMMARY

Cross-Table Themes and Insights

In small-group workshops, participants discussed core challenges and surfaced actionable ideas to close detection gaps, align global strategies, and adopt next-gen technologies. While each table explored different use cases, **six unifying themes emerged:**

1. Evolving Evasion Tactics

- Maritime “shadow fleets” are smuggling sanctioned oil via ship-to-ship transfers and fraudulent documentation, including falsified origin certificates (e.g., oil claimed as Kazakh via the Caspian Pipeline).
- Sanctioned oil is being mixed on the high seas, with insurance certificates and shipping companies complicit in the deception.
- In Mexico, oil is stolen from PEMEX and trafficked across the U.S. border, often disguised through letters of credit and shell companies at the border.
- Criminals are also exploiting legal intermediaries such as brokers, lawyers, and logistics firms as “referral points” to mask ownership and intent.
- New techniques, like time zone tracking, are being used to uncover inconsistencies in transactional behavior and surface hidden connections.
- Institutions are forced to consider not just legal risk, but also reputational risk when activities fall into gray areas (e.g., Cuba is legal in Canada but not in the U.S.).

2. Data Quality and Internal Gaps

- Institutions face deep challenges validating documents like bills of lading or letters of credit, especially when processes are still paper-based and time-sensitive.
- Manual research remains the norm, with teams combing through multilingual adverse media, complex ownership structures, and fragmented internal systems.
- While external tools like Kharon are helpful, much of the diligence still falls to credit and compliance teams.
- There’s growing interest in using technology for triage and trend analysis rather than random sampling, as well as building composite risk scores from multiple data sources.
- Legacy systems relying on basic name string matching (e.g., flagging “Miranda” for “Iran”) are producing excessive false positives. More intelligent, multilingual screening approaches are needed to reduce noise and focus investigator time.

©2025 Quantifind, Inc.

3. Global Regulatory Divergence

- Jurisdictional conflicts, such as differences between OFAC, UN, EU, and UK lists, make global compliance inconsistent and often confusing.
- Some regions require adherence to terrorism-related designations (e.g., cartel-linked entities), forcing institutions to expand KYC protocols.
- Institutions frequently consult legal advisors to interpret regional mandates and resolve cross-border contradictions.
- Reputational risk is increasingly being separated from formal examiner portfolios, leaving banks to make judgment calls independently.

4. AI Readiness and Responsible Deployment

- AI is being used for L1 triage, especially for prioritizing and summarizing alerts, but institutions draw clear lines against full automation of decisions.
- Participants emphasized that AI must be explainable, human-validated, and governed by clear policies.
- AI is particularly helpful for adverse media in multiple languages, entity linkage, and initial prioritization.
- A key concern is that regulators are starting to use AI themselves, which may increase scrutiny and expectations for transparency.

5. Organizational Design and Collaboration

- Many institutions are working to collapse siloed risk functions—integrating AML, KYC, and sanctions into unified teams or functions (sometimes dubbed “SAML”).
- Legal and privacy constraints still limit formal intelligence-sharing between institutions, but participants expressed strong interest in structured collaboration frameworks for high-risk counterparties.
- New risk triggers and escalation protocols are being created internally to reflect more dynamic threat models.

6. Future-Ready Compliance Strategy

- Fintech partnerships and outsourced vendors are introducing new third-party risks, especially where infrastructure may be infiltrated by bad actors (e.g., cartels controlling legitimate services).
- As criminal organizations are newly designated as terrorist entities, existing KYC programs must be overhauled to account for different data sources and detection approaches.
- Customers expect fast, digital-first onboarding, which creates tension with traditional, manual compliance reviews.
- Participants see real-time, explainable, and tech-enabled compliance stacks as critical to keeping pace with evolving threats and regulatory expectations.

CONCLUSION

Final Thoughts and Next Steps

The **Sanctions Convergence** event, **Uniting Forces to Combat Sanctions Evasion**, made clear that institutions are eager for more agile, integrated, and proactive compliance programs. Whether it's aligning global operations, adopting explainable AI, or closing intelligence gaps, the industry is moving toward the convergence of teams, technologies, and tactics.

We're deeply grateful for your participation. Your insights will help shape our product roadmap, partner programs, and future events.

If you'd like to stay involved through follow-ups, pilots, or continued collaboration, please reach out. Together, we can make meaningful progress in the fight against sanctions evasion.

> **"AI is no longer optional. Regulators may not require it explicitly, but the volume and complexity of sanctions risk make it the only viable path forward."**
>
> Sanctions Convergence Participant