Modernizing and Strengthening Sanctions Operations

via Secondary Sanctions Screening

Davies

Executive Summary

As financial institutions face unprecedented geopolitical risk and increased volume in the digital era, sanctions screening has become both more challenging and operationally burdensome with increased volume of alerts.

Customers transact across jurisdictions and multiple accounts, with the speed and volume of fund movements challenging traditional sanctions screening frameworks. As a result, banks, fintech, payment firms, and money service businesses (MSBs) must process millions of customers and transactions daily while managing sanctions risk and maintaining regulatory alignment.

This growing scale puts pressure on financial institutions to improve the efficiency and efficacy of their sanctions screening controls:

Efficiency
focuses specifically, to materially reduce false positives so that operational teams can focus time and resources on the alerts that have material risk.

Efficacy
ensures that the screening process reliably detects true positives without leaving any screening gaps.

Efficiency in sanctions screening can be improved through traditional methods such as model tuning and rule-based adjustments. However, these approaches only marginally address the root problems. As transaction volumes grow, financial institutions often struggle to keep alert levels manageable. In parallel, escalating sanctions, global instability, and aggressive enforcement are pushing regulatory expectations to new heights, with a sharp focus on the integrity of screening decisions and documentation.

As a result, many institutions are now looking for smarter, more sustainable ways to enhance their sanctions screening controls using secondary sanctions screening across both onboarding and payment flows, while still maintaining full control over their data, processes, and risk decisions.

This article outlines a practical framework for introducing secondary sanctions screening. By enriching customer/counterparty data, including from outside of sanction models (such as PEP and adverse media), financial institutions can materially reduce false positives while preserving security, oversight, and regulatory confidence in today's compliance landscape.

The Operational Challenge

Why traditional alert suppressions don't work

Traditional sanctions programs utilize standard systems like in-house/vendor developed filters for sanction screening and rely on system provided configuration features such as fuzzy settings, simple rules, stop words and whitelists, to control the alert rate.

These controls rely on patterns of historically similar transactions (from same or similar counterparties) for the rules and exceptions to be able to suppress alerts.

However, with globalization and rapid expansion of digital banking, a greater number of transactions and customers with newer counterparties arrive almost daily, increasing the number of close matches (alerts). In such cases, the traditional rules and exceptions are ineffective in controlling the alert rate. Additionally, financial institutions often over-configure fuzzy controls which increases the risk of true positive alert suppression.

Data quality constraints also limit the effectiveness of rules and exceptions. Incomplete or inconsistent customer, counterparty data and transactional details significantly increases the likelihood of false-positive alerts. Missing dates of birth, inconsistent name spelling and weak identifiers force screening engines to match too broadly. Industry research suggests that 20–40% of avoidable alerts stem from poor or incomplete data quality . These challenges make false positive reduction a top priority for compliance teams seeking to improve efficiency using secondary sanctions screening while maintaining strong regulatory align-ment.

As outlined earlier, the growing volume of customer transactions has led to a disproportion-ate ratio of false positives in sanctions screening. A 2025 industry benchmark study by Alessa, KPMG, Sardine. AI, and LexisNexis Risk Solutions found that 90–95% of sanctions screening alerts result in false positives , creating a significant operational burden for financial institutions. Analysts typically spend between 5–20 minutes reviewing each alert. As a result, a team dispositioning 100 alerts daily can lose 40–165 hours of productivity every week without improving risk outcomes.

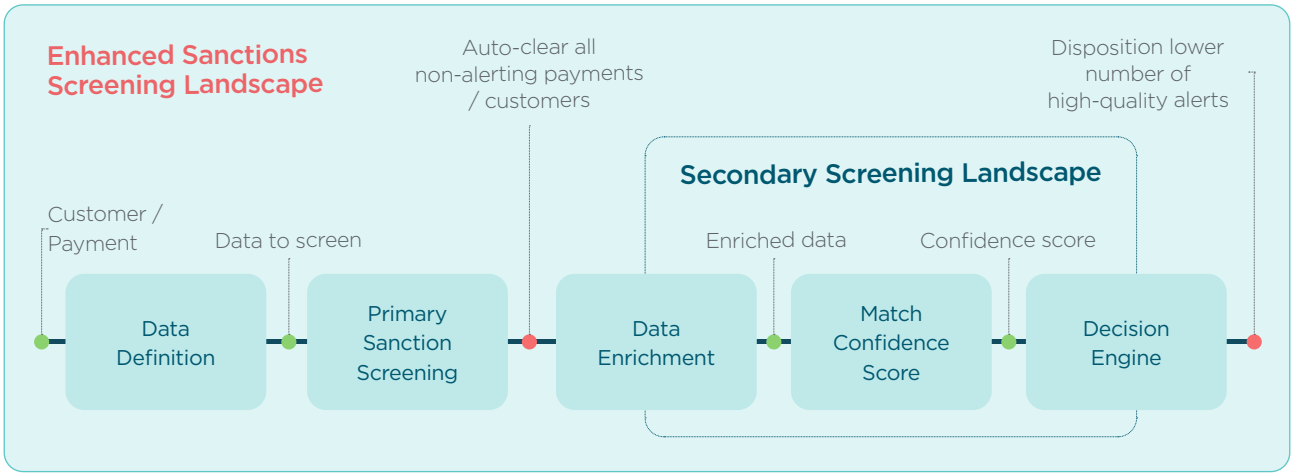
90–95%
of sanctions screening alerts result in false positives.

5–20 Mins
analysts typically spend reviewing each alert.

40–165 Hrs
of productivity a week can be lost by a team dispositioning 100 alerts daily.

Secondary Sanctions Screening Framework

Secondary screening as the name suggests is applied after primary screening but before final hits are generated in case management. Generally, the alerts from the primary screening system are passed as input to the secondary screening process to further analyse the quality of the alert.



A credible alert suppression framework relies on data enrichment and hence starts with data definition and a review of data sources to determine:

- What is available
- What is included in the current input feed to the sanctions model
- Data validation
- Data security (PII data)
- Data availability and accuracy.

Any ambiguity with the customer/ transactional data will undermine the ability of secondary screening solutions to help in alert reduction.

Data Enrichment

For customer onboarding/KYC, the primary customer screening model typically focuses on name-based matching. Secondary screening enriches the customer's data to perform a more holistic comparison. Examples of some of the enriched data elements may include:

- Date and place of birth
  Example: A name-based sanctions filter, screening a customer Mohammad Fayez living in New York city and with a DOB of May 1, 1990, will generate a false alert with a 100% match score against an OFAC SDN named Mohammad Fayez Barakat with a DOB of March 11, 1969, and living in Lebanon. With enriched date-of-birth and residence data, the secondary screening process can accurately suppress this alert.
- Government issued identifiers
  (e.g. passport numbers, national IDs, entity registration numbers)
- Current and historical addresses
- Adverse media and PEP screening

For payment screening, the process enriches counterparty information to perform a holistic comparison. Enrichment focuses on contextual and behavioural attributes, such as:

- Adverse media indicators
  related to the counterparty
- Historical transaction patterns
  including volumes, counterparties, and geographic risk
- Payment purpose
  such as unusual transaction amounts, currency flows, and high risk corridors

Data enrichment helps to produce a refined match-confidence score, which can be used as a configuration parameter, enabling institutions to suppress low-risk alerts while escalating higher-confidence matches for review.

Additionally, to aid in secondary sanctions screening, data enrichment may also focus on uncovering hidden relationships and identifying "indirect" exposure. Because secondary sanctions target entities that facilitate business for sanctioned parties, the financial institution must enrich sanctioned data with layers that go beyond simple name-matching.

Why secondary sanction screening commonly fails to achieve desired alert suppression rates:

- **Low Data Richness**
  Secondary sanction screening relies on the "richness" and "consistency" of data across records. For example, if a customer record is a missing critical identifier such as date of birth or address, the secondary screening may not have enough information to calculate a high-confidence match or dismissal.

- **Reliance on vendor provided secondary screening solutions (modules)**
  Industry standard sanction filters, sometime provide add-on modules to perform secondary screening. While these one-size-fits-all modules do work in some cases, secondary sanction modules custom built using an institution's own transaction/customer data and risk appetites and coverage, provide better and reliable result by enriching with locally available datasets and other outside datasets which may not be available in the sanctions tool.

- **Integration and Governance Gaps**
  Failures often occur during screening system/tool upgrades or migrations.

- **Lack of Feedback Loops**
  Without a process for manual reviewers to feed corrections back into the system, the secondary screening solutions may continue to make the same incorrect match decisions over time.

- **Poor Data Standardization**
  Skipping data cleaning or normalization before screening is another primary cause of failure. Inconsistent formats for names (e.g. "J. Smith" vs. "Jonathan Smith") or varying address structures can prevent the secondary screening algorithms from correctly linking entities.

How Davies can support you:

The difficulty in implementing effective secondary sanction screening solutions arises from lack of specialized expertise compared to traditional screening methods.

The secondary sanction screening solution presents unique efficiency and efficacy challenges that require in-depth sanctions knowledge. A seasoned BSA/sanctions team can execute a secondary sanctions solution in an effective manner, aligning controls for alert suppression and ensure true positives are not suppressed by over-configuration.

Davies assists financial institutions in designing and implementing customized secondary sanctions filtering solutions based on the firm's own transactional/customer data frameworks. We have a successful track record of helping institutions to reduce their alert rates by 40-50%. Our solutions incorporate strong governance controls, audit logs, customizable dashboards and reporting capabilities.

References

- https://www.mckinsey.de/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20new%20frontier%20in%20anti%20money%20laundering/The-new-frontier-in-anti-money-laundering.pdf
- https://pmc.ncbi.nlm.nih.gov/articles/PMC11621073/
- https://www.sardine.ai/whitepapers/five-ways-advanced-sanctions-screening-pays-for-itself

Author

Ramu Chandra
Principal Consultant
E: ramu.chandra@davies-group.com

Office location:

99 Madison Avenue, New York,
Ny 10016, United States

Davies US LLC

Davies US LLC. Registered office: 135 Allen Brook LN STE 101, Williston, VT

Disclaimer and Copyright Notice

1827487842_04_26_Secondary Sanctions Screening Whitepaper_V2_SK