

NR NetReveal®

Transaction Filtering

Screen transactions to entities found on internal and external watch lists with the fewest amount of false positive alerts

The challenge

- **Excessive false positives waste resources and time:** Increased alert volume places additional pressure on sanctions managers and increases their responsibility and personal liability for sanction breaches. They can't afford to let the truly important alerts slip through the cracks
- **Regulatory pressure:** New sanctions lists are released daily and the entities on these lists change fast. Screening against the correct entities all the time is a must. Recently, a bank was fined \$8.9 billion for sanctions breaches. Additionally, other banks were afraid to conduct business with them. They can't afford to let the truly important alerts go unnoticed
- **Escalating cost of compliance:** Managers and investigators are facing a steep increase in sanction designations, increasing transaction volumes, and more customers. New payment initiatives require 24/7 screening solutions and infrastructure.

Our approach

The NetReveal® Transaction Filtering solution helps financial institutions meet payment screening requirements and provides a packaged, configurable, risk-based approach for watchlist investigators to easily facilitate regulatory reporting, transaction interdiction, and asset freezing.



Our capabilities

The NetReveal Transaction Filtering solution provides financial institutions with:

Scalable global regulatory compliance

SWIFT 2021-certified application includes protocols for any message type, including SWIFT MT and MX, ACH, and FedWire. Full support for ISO-20022

Realise up to 83% reduction in false positives

Achieve up to an 83% decrease in false-positives your investigators have to review using our Match Exclusion technology. Our advanced algorithms reduce false positives on average by 40-60%

Look beyond the matches

Intelligent Event Triage auto hibernates or escalates alerts. Escalated alerts are enriched and their priority determined to make the most of an investigation team. Advanced post processing looks beyond the name match and into the context, history and risk of the transaction

Increase detection accuracy

Synonyms and Weighted Words further reduce false positives and increase detection accuracy. Associated lists of words (nicknames, similar terms, financial terms) detect more variance and focus on what is important (weights)

Flexibility to enhance scenarios

Achieve higher accuracy and better false positive performance using our Built Your Own Algorithm feature. Users can use our standard algorithms as a basis to create their own, matching their data and their specific use cases.

BAE Systems named a "Category Leader" in the Chartis Financial Crime Risk Management Systems: AML and Watch List Monitoring 2019 Vendor Landscape report



Reduce false positives against increasing transaction volumes

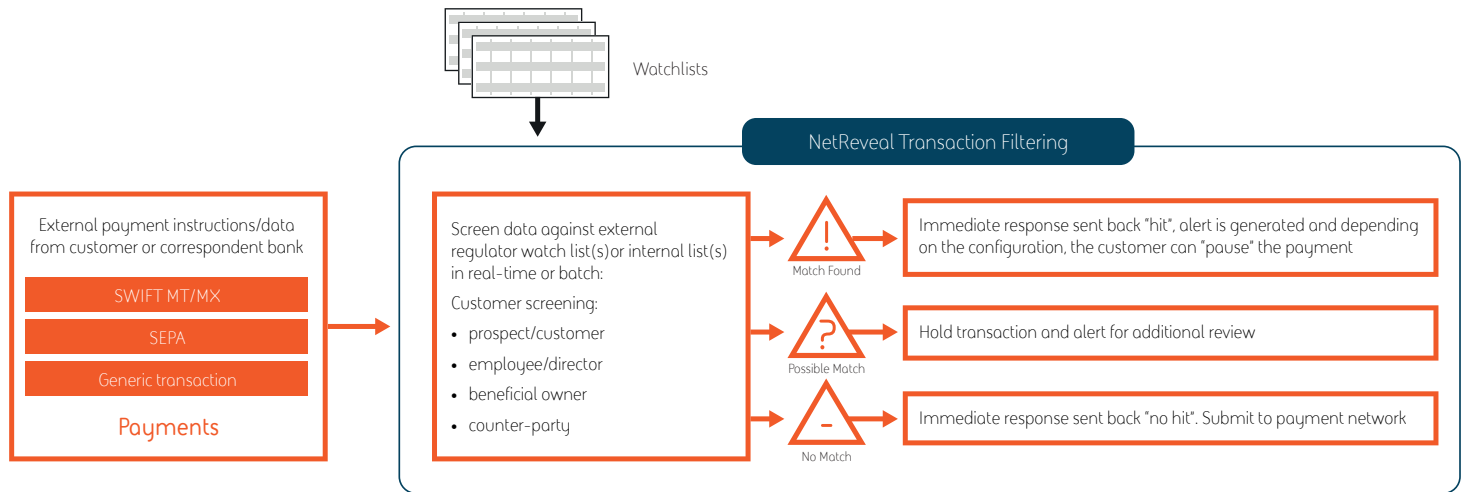
Prioritise alerts and hibernate low value
alerts for quicker alert disposition



Additional Capabilities

| Feature | Benefit |
|---|---|
| SWIFT 2021 certified app | Stay ahead of regulation with SWIFT 2021 Standards update and certification |
| Advanced detection technology | Applies specific detection logic for transaction types, geographies, and counterparties to detect different forms of data within financial transactions, such as names, addresses, dates, numeric details, or free text information |
| Identify entities with purposely altered names | Concatenated fuzzy name matching algorithm strengthens detection levels. Receive alerts on sanctioned entities or persons that have intentionally included too many or removed spaces to avoid detection by screening systems |
| Integrated view of risk history | Anti-stripping enables your investigators to screen alerts against previously blocked payments |
| Maximise screening model efficiency | Our Versioning feature allows users to adapt detection configurations easily and find what works. Investigators can store multiple versions of a detection configuration in the model repository then choose the model to deploy for screening |
| Factor in market implications | Currency Cut-off prioritises currency based on market to enable legitimate transactions |
| Automated updates | Lists are automatically imported and updated daily or even multiple times per day to ensure institutions are screening against the most up-to-date lists to reduce exposure across their organisation |
| 24x7 architecture | Architecture separates processing from the user interfaces to ensure maximum resilience, stability, and scalability |
| Intuitive user experience | Facilitates interdiction workflow, follow up reporting, and regulatory disclosure for more efficient and effective investigations |
| Single enterprise-wide deployment supporting multiple lines of business | NetReveal is capable of being deployed across organisational international group-wide segregated hierarchy. Field-level security through the NetReveal Data Privacy Agent enables institutions to comply with local data privacy regulations |
| Capitalise on real-time and batch processing | Supports 350+ global watch lists and performs advanced screening against millions of watchlist entries. Send payments to our system through JMS, SOAP, REST, HTTP or Kafka and get the responses very fast. Our solution works fast enough to handle instant transfer or payment protocols. Deliver batch files or link your payments database for fast batch processing. |

How it works




External payment data is captured into the system for screening against external regulator watch lists or internal lists then transactions are classified as "match found," "possible match," or "no match." Transactions can then be paused, held for further review, or released to payment network.


BAE SYSTEMS

Contact Details: UK: +44 (0) 330 158 3627 | US: +1 720 696 9830 | AUS: +61 290 539 330

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/NetReveal

 linkedin.com/company/baesystemsai

 twitter.com/baesystems_ai

Copyright © BAE Systems plc 2021. All rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No. 1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.