

Compliance Customer Screening

How You Can Reduce
False Positives With
Intelligent Matching

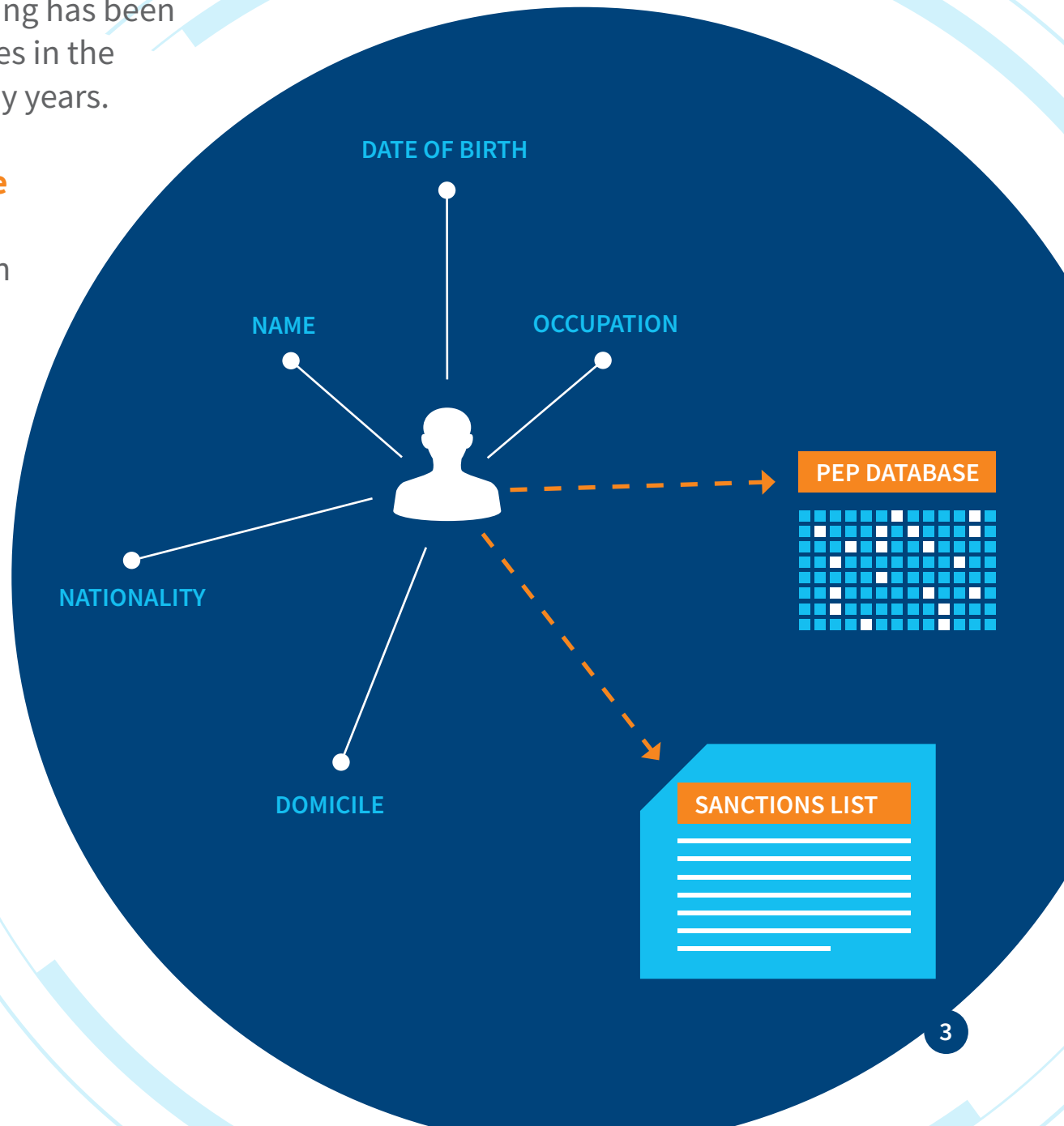
As Anti-Money Laundering (AML) compliance requirements expand into various areas, so do the number of alerts that must be manually researched. This makes weeding out false positives increasingly—and frustratingly—necessary.

To be in compliance with AML and Counter-Terrorism Financing (CTF) processes, corporations must screen customers and transactions against various lists. As those lists and compliance obligations grow, so do the number of matches or near-matches that must be manually investigated. The investigations can be complicated and time-consuming. A vast majority of alerts prove to be false positive. Companies with millions of customers to screen can find the costs of compliance oppressive. This makes the need to reduce the number of false positives a priority.

LexisNexis® Intelligent Match Decision Solution is built to solve this false positive problem—[click here](#) to learn more about how it enhances LexisNexis® Bridger Insight® XG.

Automated matches generate alerts

Know Your Customer (KYC) screening has been a key part of AML and CTF processes in the financial services industry for many years. Customers are screened against a variety of **compliance intelligence information**, including sanctions lists and Politically Exposed Person (PEP) databases. A variety of characteristics such as name, date of birth, nationality, domicile, occupation, etc., constitute an organization's customer **data profile** and the records of individuals and business partners maintained in its compliance intelligence databases.






An automated match between a customer profile and a compliance intelligence profile generates an alert for manual review. KYC screening is carried out initially as part of the onboarding process and is repeated throughout the customer journey. Rescreening might be triggered by changes to the customer data or intelligence information. It may also be performed periodically in accordance with AML risk management policies.

This initial and ongoing screening is a constant, resource-intensive process, requiring sophisticated systems to carry out automated matching as well as significant human resources to review the system-generated alerts. In an era in which the scope of AML control activities is constantly expanding, process **efficiency has become a key objective** for most compliance departments.

Many organizations find their current manual review of alerts to be disproportionately costly as compared to the perceived risk-management benefits of the overall screening process. As a result, there is **increasing pressure on AML systems managers to reduce false positive results**—the alerts generated by the system that are ultimately discarded during the manual review process because of the absence of a true financial crime risk.

Learn how LexisNexis Intelligent Match Decision Solution can help you meet increasing compliance demands and protect your organization from regulatory exposure without draining resources from your core business activities.





In addition to tying up valuable compliance resources, false positive alerts may also create friction for innocent parties whose financial activities might be disrupted while false positives are investigated. Excessive volumes of false positive results may even contribute to AML risk. Staff members reviewing the alerts may be more likely to overlook a true match while working through a sea of false positive alerts.



Organizations facing these challenges ask: What factors contribute to the generation of false positive results? And how can these factors be managed to improve the effectiveness of AML screening?

Approach to false positive reduction

The following considerations should be kept in mind when attempting to reduce false positive results.



Invalid vs. Valid False Positive Results

The distinction between invalid and valid false positive results can't be overlooked when attempting to reduce overall false positive results. Such exercises frequently focus on invalid false positive results, but efficiency gains can be greatest if both categories are considered.



Invalid false positive results are those in which the customer records and compliance

intelligence details—as presented to the matching engine—do not suggest that the two profiles matched in an alert relate to the same party. They represent a failure of the matching logic.

The failure may be due to “fuzzy” matching algorithms that matched two names that are not in fact similar, or because other characteristics indicate that the profiles belong to two distinct parties, such as one in which the dates of birth vary significantly, or in which, for example, one party is a teenage customer in one country and the other is a senior politician in another.

Addressing rates of invalid false positives requires a careful assessment of the matching technology used and its configuration to ensure any changes made do not have unintended negative consequences.



Valid false positive results are those in which the details—as presented to the matching engine—indicate that they may relate to the same party, but upon investigation are found to be unrelated. This situation typically occurs because key characteristics such as name and approximate ages of two distinct parties are similar. While the number of common names in use around the world certainly presents a challenge, some gains may be made by ensuring that the populations being screened against each other do not contain redundant or obsolete profiles.

Other matches that are later found to be unrelated may be the result of sub-optimal data quality or structure that prevents the matching engine from identifying characteristics that distinguish the two parties. The latter can be addressed by examining the underlying flaws in the data being screened (either on the customer side or on the compliance intelligence side).

Find out how LexisNexis Intelligent Match Decision Solution can help identify and clear false positives.



Risk Appetite

Throughout any efficiency drive, a reduction in hit rates should not be the only objective. All organizations should have a clearly defined **screening tolerance standard**—approved by senior management—from which those responsible for configurative changes can work.

This standard should dictate the types of profile match that management expects to generate—a screening alert. It should also outline the kind of matches management does not want forwarded to the manual review process. Systems managers are then free to adjust the precision of matching algorithms within the limits set by the screening tolerance standard.





Documentation

Throughout any exercise to improve the efficiency of screening programs, **risk-based justification** should be clearly documented for all configurative changes. Projects to reduce false positive alerts



are usually initiated as a result of operational, budgetary or regulatory concerns so conclusions tend to be driven and documented from the point of view of resource implications.

However, the risk of increasing **false negative results** (dropping true alerts) should also be considered part of the exercise. At best, it may result in negative reviews from regulators or auditors, and at worst, it may lead to relevant matches being dropped from the screening process.



LexisNexis Intelligent Match Decision Solution is built to help solve this false positive problem—[click here to learn more.](#)

Intelligent Match Decision Solution is a fully integrated tool in LexisNexis® Bridger Insight® XG that enables better, more sophisticated decisions defined at the attribute level, yielding a higher percentage of automatically remediated matches.

For more information, call 800.658.5638 or visit risk.lexisnexis.com/products/intelligent-match-decision-solution



About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

This e-book is provided solely for general informational purposes and presents only summary discussions of the topics discussed. This e-book does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this e-book.

LexisNexis Intelligent Match Decision Solution provided by LexisNexis Risk Solutions is not provided by “consumer reporting agencies” as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) (FCRA) and does not constitute a “consumer report” as that term is defined in the FCRA. LexisNexis Intelligent Match Decision Solution may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA. Due to the nature and origin of public record information, the public records and commercially available data sources used in reports may contain errors. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Copyright © 2020 LexisNexis Risk Solutions. NXR14285-00-0220-EN-US