

GETTING TO KNOW YOUR CUSTOMER THROUGH RELATIONAL RISK ASSESSMENT

Part 3 of a 3-part series on anti-money laundering technology.

Neil Katkov, PhD

CONTENTS

- Background 1
- Introduction..... 2
- Holistic AML 4
- Relational Risk Assessment..... 5
- Resolving Challenges in AML Compliance 7
- Conclusion..... 9
- Leveraging Celent’s Expertise 10
 - Support for Financial Institutions 10
 - Support for Vendors 10
- Related Celent Research 11

BACKGROUND

This report was commissioned by Accuity; however, the analysis and conclusions are Celent's alone, and Accuity had no editorial control over report contents.

Accuity offers a suite of innovative solutions for payments and compliance professionals, from comprehensive data and software that manage risk and compliance, to flexible tools that optimize payments pathways. With deep expertise and industry-leading data-enabled solutions from the Fircosoft, Bankers Almanac and NRS brands, our portfolio delivers protection for individual and organizational reputations.

Part of RELX Group, a global provider of information and analytics for professional and business customers across industries, Accuity has been delivering solutions to banks and businesses worldwide for 180 years. For more information visit accuity.com.

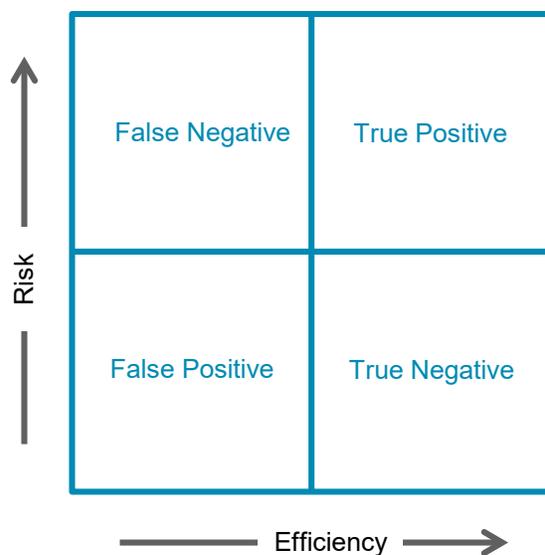
INTRODUCTION

It is often said that banking is a relationship business. The same can also be said of anti-money laundering (AML) compliance, where rooting out suspicious entities is largely a matter of uncovering alliances that hide illicit activity.

As noted in the first paper in this series, identifying risky actors is a core mission of AML programs. Traditional approaches to this crucial task rely on screening entities against watchlists, news media, and other data sources. This approach may flag customers appearing on watchlists or in negative news, but it has two key, complementary limitations:

- **False positives:** Watchlist screening, whether for know your customer (KYC) or sanctions and payments screening purposes, typically generates high rates of false positives. Processing these false positives has been the leading factor behind the skyrocketing costs of AML compliance over the past decade.
 - Processing high rates of false positives is a low risk / low efficiency approach to AML. It plays it safe by examining more alerts, but the price financial institutions pay for this is high operational costs.
- **False negatives:** Simply put, bad actors and high-risk entities routinely slip through screening and KYC checks. Sophisticated malefactors develop elaborate schemes involving multiple entities and accounts to elude detection. At the same time, screening operations may not always make full use of available AML tools, leaving financial institutions exposed.
 - Traditional AML approaches that fail to identify bad actors both subject the institution to high risk and at the same time fail to create sustainable operational efficiencies.

Figure 1: The false positive / false negative problem



Source: Celent

The goal for AML compliance, then, is to both accurately categorize the true negatives (business as usual customers) as well as to identify the true positives (bad actors) for referral to regulators and law enforcement.

Financial institutions thus face a serious challenge within their AML operations: increasing the accuracy of their entity screening to reduce false positives, while at the same time minimizing the number of high-risk entities that slip through the net. Uncovering hidden relationships are key to this effort, and technology can help.

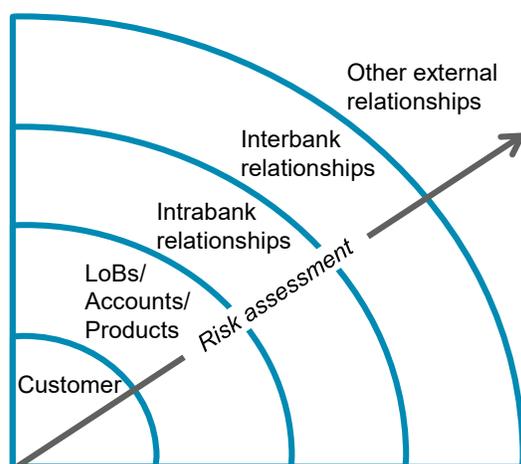
HOLISTIC AML

Understanding relationships is key to assessing the risk an entity poses, and this starts with understanding the entity's relationship to the bank. Money launderers, fraudsters and other high risk entities have or seek to establish multiple account and product relationships through which to channel funds licit or illicit. This may involve accounts and activity across different lines of business of the bank, as well as across the bank's operations in other states or countries.

For this reason it is important for a bank to have a holistic view of its customers' account relationships across lines of business, products, and geographies in order to accurately understand customer profiles, activity, and potential risk.

Taking things a step further, banks need to understand relationships and linkages among different customers and accounts as well as activity between accounts. Finally, a full view of risk will involve understanding the links between a bank's own customers and their accounts and counterparties at other institutions, including other geographies.

Figure 2: Peeling the onion: a schema for Holistic AML



Source: Celent

In this way, achieving holistic AML requires implementing the capability to undertake enterprise-wide analysis of its customers, accounts, activities, and counterparties both within and external to the bank. This will involve:

- **Coordinated AML programs** across a firm's operations.
- **Enterprise-wide data management** to enable access to customer, account and transactional information across siloed lines of business and geographies.
- **AML analytics** to identify and examine links among customers, accounts, and counterparties.
- **A Financial Investigation Unit (FIU)** supported by technology and tasked with resolving high-risk cases.

A holistic view of accounts and activity allows a bank to better understand its customers' relationships and linkages. Yet many account relationships and activity are perfectly above-board. To separate the suspicious entity from the legitimate customer further requires the ability to understand the risk inherent in these relationships.

RELATIONAL RISK ASSESSMENT

Entity screening is perhaps the fundamental tool for assessing customer risk. Screening only against official watchlists, however, will inevitably provide a one-dimensional view. Moreover, watchlist screening is notoriously susceptible to generating high rates of false positives. Developing a fuller risk picture of the entity requires screening against many external data sources, including public records data, as well as understanding the entity's "public presence" in news media, including negative and positive news.

Still, screening a single entity against these data sources, no matter how voluminous, does not provide the fullest picture of the entity's potential risk. This fuller view, a true 360 degree view, comes from understanding the entity's associates and relationships and, moreover, assessing the risk inherent in those relationships.

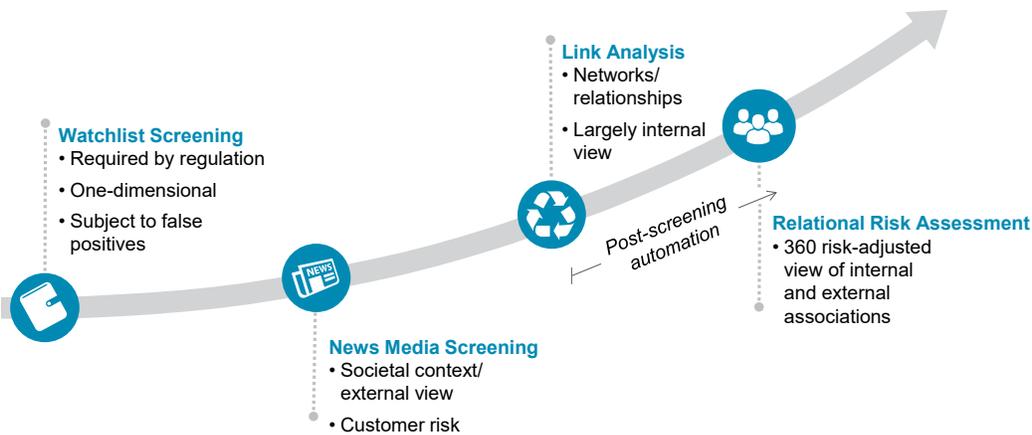
The relational risk assessment approach takes link analysis several crucial steps further. Link analysis, a feature of numerous AML software solutions, maps out connections between customers, accounts, and transactions and renders this network visually. This useful tool allows analysts to intuitively scrutinize related accounts, cash flows between entities, and other linkages in their search for suspicious activity. There are, however, a number of limitations to traditional link analysis:

- Because link analysis is performed on accounts and transactions within the bank, it provides a largely internal view of activity. Transactions with external counterparties may be captured, but other external relationships that may hide risk will not be.
- Link analysis is good at identifying account relationships and nodes of activity, but does not assess the risk level of these accounts or external counterparties. Due diligence on associated entities is left to the analyst to perform.
- Link analysis auto-generates network maps, but interpretation of the network is largely a manual due diligence process.

Similarly, screening against news media and other data sources may uncover associates and relations of an entity, but does not assess the risk in those relationships. This work must also be performed by the analyst.

Relational risk assessment goes beyond both link analysis and news media screening. The approach not only seeks out the connections between an entity and other parties, but also performs a risk assessment on those related entities. Such connections need not always be direct links between two entities; meta-relationships, such as both entities appearing in a public record or other shared context, can also indicate risk. In a variant of guilt-by-association, a customer with ties to high risk entities will itself be placed in the high-risk category. Moreover, this assessment is performed automatically through advanced analytics.

Figure 3: Risk assessment techniques



Source: Celent

Importantly, an analytics-based approach to assessing the risk of an entity by also examining the risk inherent in the entity's circle of relations and associates can work to reduce *both* false negatives and false positives.

- False negative reduction: By identifying and examining an entity's associates, relational risk profiling can uncover risk factors that would go unnoticed by single entity screening or link analysis.
- False positive reduction: Conversely, this fuller view of customer risk can help a bank to identify and prioritize high risk entities with more confidence and relegate the low risk customers to the true negatives pile.

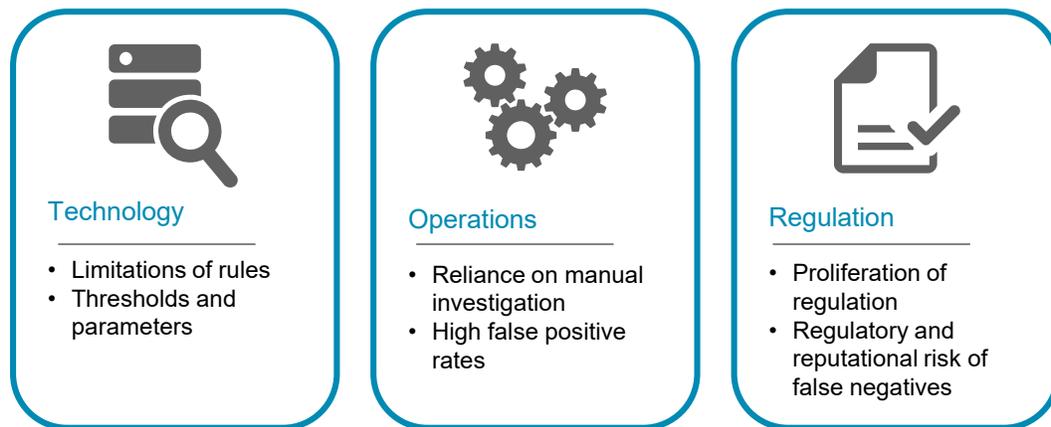
The significance of leveraging analytics to perform this analysis cannot be overstated, for several reasons:

- Due to its highly manual nature, customer due diligence (CDD) work is a major factor in the steady increase in analyst teams and the crippling cost of AML compliance. Analytic platforms can automate much of this work.
- The ultimate reason for soaring compliance costs is the need to process ever higher numbers of false positives. Analytics-based relational risk assessment can reduce the number of false positives, and hence the operational burden, significantly. Moreover, analytics can achieve this through a highly efficient, automated process.
- Analytic platforms not only add efficiency through automation, they are able to uncover relationships and risks that a human analyst might never detect. This is due both to the sophisticated algorithms used in advanced analytics as well as the large number of customers, external entities, and data sources that must be correlated.

RESOLVING CHALLENGES IN AML COMPLIANCE

By providing an additional dimension to capture, segment, and prioritize risk levels, relational risk assessment based on advanced analytics can help reduce the false positives generated by traditional screening methods. This approach can also be effective in automating much of the post-screening investigative process. These capabilities make it a powerful tool in addressing some of the intractable challenges and shortcomings of current screening and KYC technology.

Figure 4: Challenges in AML compliance



Source: Celent

- **Challenges with rules.** Although they have been the mainstay of AML screening and monitoring technology, rules are a fairly blunt tool to assess risk. Rules are prescriptive by nature and must be written for every specific risk factor. This limits their ability to spot novel risks, while at the same time casting a wide net that invariably scoops up many licit actors, generating large numbers of false positives.
 - Advanced analytics techniques including statistical analysis, predictive analytics, and link analysis are an effective way to supplement (or replace) rules-based methodologies to overcome these limitations. Analytics provides twin benefits in 1) discovering risks that rules-based systems and manual analysis cannot uncover, while 2) increasing the accuracy and efficiency of AML compliance operations through greater automation.
- **Challenges with thresholds.** Achieving the right balance with thresholds can be a struggle. Setting parameters too loosely will result in high false positive rates; conversely, tightly wound variances will let too many risks slip through the net. This is a particular danger in KYC and CDD, where it may be advisable to screen customers with no thresholds to maximize risk capture. This will inevitably produce false positives.
 - Running relational analytics on screening results can resolve many of these alerts by identifying the truly risky actors based on their social and professional context and associations. Entities that lack such contextual indicators can be more safely treated as business as usual, low risk customers.

- **Operational challenges.** From an operational perspective, the swelling analyst teams needed for manual investigation — largely a matter of resolving false positives — is the largest pain point in AML compliance.
 - Risk assessment leveraging analytic platforms can achieve significant reduction in false positives and help relieve this operational burden.

Most screening and link analysis techniques still leave too much work to the analyst. Smart analytics can assess the risk of entities and associates, taking over much of the work typically performed by analysts. Moreover, capturing the full risk picture of an entity and its environment, which includes risk assessment of the entity's associates and relationships, can shine a light on risky entities that might otherwise elude detection.

CONCLUSION

Relational risk assessment is based on an intuitively suggestive premise: that a full view of customer risk will analyze not just the risk of the entity itself, but also the risk of individuals and companies with which the customer is associated, related, or linked. Augmenting current AML technology by adding this additional layer of analysis to screening methodologies can help alleviate some of the thorniest issues in AML compliance.

In a world of soaring compliance costs where false positives may reach 70 percent of alerts, relational risk assessment techniques have achieved false positive rates under five percent or even one percent. This in turn enables operational efficiencies and frees up analysts to perform more value-added compliance work. Moreover, by enhancing the accuracy and confidence level of risk assessments, this approach can help keep a firm's regulatory and reputational risk in check.

These are significant benefits. Watchlist screening arguably draws the most regulatory scrutiny of any area in AML compliance. The largest AML compliance fines levied against banks have been due to issues with screening operations.

Moreover, as described in the first part of this series on anti-money laundering technology, watchlist screening is an integral part of every facet of AML operations. Screening supports entity review from onboarding and risk profiling to customer review; payments screening including sanctions and domestic payments; and forensics including enhanced due diligence, detection, and risk prevention.

Faced with ever-increasing regulatory requirements and burgeoning AML compliance costs, financial institutions are keen to offset the growing burden with operational efficiencies. Firms are looking to supplement, and in some cases even replace, their existing AML technology stack with advanced technologies to achieve greater automation, efficiency, and accuracy.

In an era of rapidly evolving technology and a fast moving ecosystem of Regtech startups, relational risk assessment powered by advanced analytics has demonstrated efficacy in mitigating the challenges of watchlist screening operations. For many firms, this is a promising place to start the journey toward the future of AML technology.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

SUPPORT FOR FINANCIAL INSTITUTIONS

Typical projects we support related to anti-money laundering compliance include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

SUPPORT FOR VENDORS

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials — including your website and any collateral.

RELATED CELENT RESEARCH

Innovation in AML Technology: New Tools for Optimizing Compliance Efficiency

November 2017

Innovation in Compliance Technology: Emerging Themes and Vendor Solutions

June 2017

Market Surveillance in Capital Markets: The Growing Role of Artificial Intelligence

August 2016

Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency

August 2016

Onboarding in Corporate Transaction Banking: Prioritizing Investments for Reducing Friction

August 2016

Emerging Solutions in Anti-Money Laundering Technology

April 2015

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

Copyright © 2018 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman (“Celent”) and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner. This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent’s rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

For more information please contact info@celent.com or:

Neil Katkov, PhD

nkatkov@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucril Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059

South Korea

Youngpoong Building, 22nd Floor
33 Seorin-dong, Jongno-gu
Seoul 110-752

Tel.: +82.10.3019.1417
Fax: +82.2.399.5534