

REPRINT

R&C risk & compliance

SEGMENTATION AND AI IN AML ALERTS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2019 ISSUE



www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

NAVIGANT

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com
© 2019 Financier Worldwide Ltd. All rights reserved.



R&C risk &
compliance

www.riskandcompliancemagazine.com

MINI-ROUNDTABLE

SEGMENTATION AND AI IN AML ALERTS



PANEL EXPERTS**Alma Angotti**

Managing Director

Navigant

T: +44 (0)738 702 730

E: alma.angotti@navigant.com

Alma Angotti is a managing director and co-head of the Global Investigations & Compliance practice at Navigant. With over 25 years of regulatory practice, Ms Angotti has held senior enforcement positions at the SEC, Treasury's Financial Crimes Enforcement Network (FinCEN) and FINRA (Financial Industry Regulatory Authority). In these positions, she was responsible for conducting investigations involving securities fraud, insider trading, financial fraud, anti-money laundering (AML) and counter terrorist financing, market manipulation, investor and market protection, and other regulatory violations.

**Salvatore LaScala**

Managing Director

Navigant

T: +1 (212) 554 2611

E: salvatore.lascalas@navigant.com

Salvatore LaScala is a managing director and co-head of Navigant's Global Investigations and Compliance Practice in New York, NY. Possessing a broad range of subject matter knowledge and expertise, Mr LaScala applies his 20-plus years of hands-on experience to conduct investigations and compliance reviews on behalf of financial institution clients responding to regulatory or law enforcement matters concerning anti-money laundering, the Bank Secrecy Act, the USA PATRIOT Act and the Office of Foreign Assets Control.

R&C: Could you provide an overview of how technology is transforming financial institution's (FI's) anti-money laundering (AML) processes?

Angotti: Technology enhancements in financial institutions (FIs) are becoming indispensable to managing financial crime risk. Regulators expect FIs to make use of the enormous amount of data they have about their customers and their customers' transactions. The only way to effectively identify risk from all of this data is through technology. The United Nations Office on Drugs and Crime estimates that money laundered globally is about 2-5 percent of world GDP annually, about \$3 trillion. In addition, the number of noncash transactions will increase as mobile technology – mobile wallets and mobile money transfers – are introduced into the global market and emerging markets. For the past few years, FIs have wrestled with methods to minimise loss, remain efficient and maintain proper regulatory compliance. Technology is transforming FIs' anti-money laundering (AML) processes by efficiently sorting through large amounts of data, developing more useful predictive modelling and using client segmentation and behavioural patterning. Technology has the potential to better identify risk, by eliminating some of the 'noise' in the data and by enabling compliance personnel to concentrate on actual risk.

LaScala: Over the past few years, FIs have begun to embrace robotic process automation to expedite their more tedious work. This is achieved by either business process automation or by using 'bots' designed to perform automated and repetitive tasks. As such, AML analysts and investigators derive increased efficiencies and get to focus on the AML typologies, rather than gathering and exhibiting investigative artefacts. This shift in focus results in increased quality, productivity and employee satisfaction. At the same time, tremendous strides in artificial intelligence (AI) and machine learning (ML) are working to increase the quality of AML alerts while decreasing the volume. Access to this broader collection of cognitive tools, which have evolved significantly in recent years to include ML, deep learning and advanced cognitive analytics, will, no doubt, yield remarkable benefits relating to the effectiveness and efficiency of AML transaction-monitoring systems.

R&C: With AML departments sifting through many alerts to pinpoint suspicious activity, can you outline specifically how artificial intelligence (AI) and segmentation help FIs to avoid wasting time and effort on too many low value alerts?

LaScala: FIs typically interrogate activity of one large business without segmenting that business

into the different kinds of customers. For example, in retail banking, there might be 'premium banking', which covers students, recent graduates and middle-class to upper-middle-class-income customers, with a split only at the 'private banking' level. This can result in applying only one set of rules with one set of parameters to all the 'premium banking' customers. Applying AI to the 'premium banking' segment can result in the identification of four or five separate subgroups of customers that behave similarly and, as a result, now have their own segments. Customising the parameters of the detection scenarios to each of those additional segments, in our experience, has resulted in significant efficiencies by reducing the false positives caused by applying one set of detection scenario parameters to very diverse groups. Segmenting and customising the scenarios has been shown to identify previously undetected suspicious transactional activity with many fewer false positives. This combination of more effective and more efficient monitoring is our goal.

R&C: What should be the key strategic considerations for FIs when using AI as part of the AML alert process? How would you characterise the importance of AML alert analysis along the suspicious activity decision chain?

Angotti: The AI process requires a strategic approach. Regulators need to see a clear objective; therefore, it is important that an FI start small. The FI should target specific areas with proper testing

"The AI process requires a strategic approach. Regulators need to see a clear objective; therefore, it is important that an FI start small."

*Alma Angotti,
Navigant*

and controls. Second, be transparent. Regulators and auditors need the opportunity to access and understand the solutions that have been provided. Third, be effective. The AI must efficiently and effectively address the risks and concerns of the FI and provide apparent improvements. Next, the institution should document a clear justification for the results of the AI. Subject matter experts (SMEs) must support, review and test the results. The FI must utilise technology with an industry-proven and vetted track record. Lastly, the AI should not be considered a replacement for investigators, analysts and quality assurance professionals, but rather AI should support them. This strategic AML analysis plays a very

important role along the suspicious activity decision chain. The data captured through the AML process is used to justify and develop the potential suspicious activity report (SAR). Therefore, it is important that the AML process employ a strategic approach when analysing suspicious activity.

R&C: What transaction data is typically utilised in the AML alert analysis process? What key data needs to be made available to the recipient of an analysis, such as an auditor or regulator?

LaScala: The transaction-monitoring systems consume many data points to generate alerts. In some respects, it is better to define which information not to include, which might consist of automatic, accounting or administrative financial events. Nearly everything customer-activated is in scope. Deposits, withdrawals – by cash, check, monetary instrument, wire or automated clearing house – are just a few. Transaction codes, product codes and any predetermined risk codes or industry designations are also frequently consumed. In addition to the transactional data and the transaction codes, customer reference data is key. This can include account name, number, opening date, closing date, occupation, politically exposed person status, and more. Additionally, the

list of products the customer uses, such as custody, trading, online banking, remote deposit capture and international wires impact transaction monitoring. All the data above will be used by an astute investigator or analyst to disposition an alert. In fact, typically all detection scenario alerts are reviewed to ensure that the data points that compose them were appropriately identified. If any of the data points were not appropriately identified, the alert could be a false positive. When the investigator disposes the alert, he or she should be working from a defined investigative protocol specific enough to be tested. Moreover, the documentation included to support

“Segmenting and customising the scenarios has been shown to identify previously undetected suspicious transactional activity with many fewer false positives.”

*Salvatore LaScala,
Navigant*

the alert should consist of enough exhibits for a third party to repeat the work and come to the same conclusion as the investigator. As such, other stakeholders such as internal audit or examiners

should receive the entire investigative file and the exhibits prepared by the investigator.

R&C: In what format should alerts and resolutions be presented to an auditor or regulator in order to reduce the number of analysis failures? To what extent are alert analysis failures a root cause of AML problems?

Angotti: AI can help make the alerts more productive, but alert analysis will continue to be heavily dependent on SMEs evaluating the output – that is, identifying suspicious activity. Transaction monitoring is a combination of people, processes and systems. Alert analysis failures sometimes do contribute to the failure to identify risk. If the FI is not properly trained and lacks robust documented processes, protocols or decision matrices, then the analysts may not properly identify the risk of the alerted transactions. In addition, the FI must institute a good quality control programme, to make sure the analysts are following the procedures, and a good quality assurance programme to make sure the procedures are fit for purpose. Institutions need to focus on those aspects of the programme to show regulators that the current Bank Secrecy Act (BSA) or AML programme can effectively identify transactions or accounts that may be suspicious and reportable.

LaScala: Alerts and resolutions or dispositions should be given to an auditor or regulator with the investigative protocols that the investigator used for the case. Additionally, the investigative memo and any exhibits should be provided in one physical or electronic folder. If stored electronically, the exhibits should have standard naming conventions to facilitate review. In essence, provide the reviewers everything they need in a very organised fashion so that they can focus on the analysis rather than being distracted by trying to figure out the process.

R&C: What steps should FIs take to develop an action plan that allows them to research and resolve AML alerts and maximise the effectiveness of their AML protocols?

Angotti: AI requires human tuning and input and human analysis of the output. Data scientists and SMEs must work with AI to test and tune it appropriately so that it works as intended. The FI should prioritise two things: first, analysing the high-quality alerts, and second, creating a symbiotic relationship between the SMEs and the domain experts. The FI should prioritise the most productive alerts produced by AI because AI and intelligent segmentation are able to identify behavioural patterns that traditional transaction monitoring is not. The domain experts alongside the SMEs should play a leading role in assessing the relevancy of

the data used by the AI. If the integrity of the data input into the AI is inadequate, the AI output will be inadequate and create low-quality alerts. The priority should be on building a team of data scientists and SMEs who work in conjunction to create an efficient and effective BSA or AML AI programme. The overall process needs to be connected throughout.

R&C: Going forward, do you anticipate segmentation and AI will continue to improve AML processes? What innovations are in the pipeline?

Angotti: Intelligent segmentation and AI will improve as they become more mainstream. Eventually, intelligent segmentation and AI will become more widely recognised and they will not only become a requirement in the financial services industry, but regulators will begin to expect intelligent AI as a best practice in compliance. Segmentation will

also become smarter as technology focuses more on behavioural and transactional patterns instead of traditional static coarse segments. Data scientists and SMEs will continue to improve supervised and unsupervised ML through tuning and evaluation. For example, the initial review of alerts may be completed by AI with little to no human interaction. Human analysts can then review the alerts most likely to identify true risk.

LaScala: We have only just begun to exploit the insights to be gained by AI in the AML process. It is important to proceed with highly documented and transparent protocols to help ensure the continued support of regulators and law enforcement. Cloud-based software can potentially answer millions of questions by scanning financial information, as well as drug approvals, economic reports, monetary policy changes and political events. The possibilities are endless. **RC**