Ovum
TMT intelligence | informa

Oracle looks to provide a window to the black box to drive AI into anti-money laundering

Publication Date: 13 Nov 2017 | Product code: ENV004-000001

Daniel Mayo

Ovum view

Summary

While machine learning (ML) is a well-established tool on the fraud detection side of anti-financial crime, its use on the anti-money laundering (AML) side has been more problematic. This is particularly true in the US, where supervisory agencies have tended to adopt a rule-based – rather than risk-based – approach, with a low tolerance of detection failures. Consequently, "black box" ML systems are generally not used for frontline purposes, because they do not provide the "why" behind an alert generation. While technically effective, a lack of regulatory support means they have limited value.

Oracle is looking to address this issue by providing a tool within its Financial Services Anti Money Laundering platform that generates this supporting narrative. The tool will pictorially explain which variables contributed to a decision process so that a local observation can be explained. This is an important step that should help drive regulatory support for wider ML-based approaches to compliance.

Regulators remain tough on ensuring AML detection effectiveness

While recent regulatory penalties related to financial crime compliance breaches (e.g., money-laundering or sanction breaches) have not been at the billion-dollar levels seen earlier this decade (HSBC with $1.9bn in 2012 and BNP Paribas with $8.9bn in 2014), recent fines certainly indicate that regulatory scrutiny and enforcement remain robust. The back end of 2016 saw the New York State Department of Financial Services (NYDFS) issue fines of $235m to Intesa Sanpaolo SpA and £215m to Agriculture Bank of China. Deutsche Bank was then fined $630m in January (by the NYDFS and the UK's FCA), and Western Union $586m, and the NYDFS announced at the end of August that it was seeking $630m from Habib Bank for AML failures. On top of this, while the fine has not yet been agreed, AUSTRAC (Australia's financial intelligence agency) is suing Commonwealth Bank of Australia for AML breaches, with potential fines in the billion-dollar range based on the number of cases involved.

With the EU's 4.1 Directive widening the reach of the recently implemented Fourth Anti-Money Laundering Directive, and the initial impact of the Trump administration suggesting that US regulators will continue unabated in enforcement action, the focus on AML effectiveness for most banks remains unsurprisingly high. This is driving significant investment across the banking sector. Ovum's 2017/18 ICT Enterprise Insights program (published in October 2017), which included interviews with senior IT executives at more than 470 retail banks, found that across risk and compliance, AML is the area where the most institutions plan to increase IT spend in 2018. The survey also included interviews with more than 200 corporate banks, and while IT spending growth on conduct risk is higher overall, AML is one of the top areas of spending growth.

The ICT Enterprise Insights study also explored investment priorities for tackling financial crime. The top priority was improving detection rates, with increasing speed of detection and minimizing false positives and customer inconvenience also highly prioritized. The challenge for banks is to ensure that they avoid AML compliance breaches, in a timely manner, while at the same time reducing the impact on customers and retaining control of operating costs.

ML techniques can drive self-tuning, but regulatory acceptance is key for frontline deployment

Detection effectiveness can be improved with a number of steps. Firstly, banks need to conduct regular risk assessment and gap analysis of risk controls. This would assess coverage of risk factors within existing AML models to ensure such risks are adequately mitigated or controlled, as well as identify gaps in product and customer monitoring as new risks are identified.

Secondly, banks need to tune rule thresholds for automated transaction monitoring and alert systems so that alert-to-case ratios are optimized (cases are transactions where there is potentially suspicious activity that requires reviews by monitoring teams before being cleared or escalated for suspicious activity report [SAR] filings). This is achieved through statistical tuning using above-the-line (ATL) and below-the-line (BTL) testing, where rule efficiency is evaluated compared to different thresholds. Thirdly, post-alert processing analysis can be conducted to prioritize case lists and allocation for investigation to improve the effectiveness of the investigations function.

For both of these latter areas, machine-learning techniques can be used to optimize these steps automatically on an ongoing basis (as opposed to the manual periodic reviews that most banks currently do). However, while this provides some benefits, a more effective approach would be to use ML techniques to determine the rules and thresholds directly (i.e., without manual modeling and setup in which there is only periodic review of underlying variables).

The core challenge here is that ML techniques often result in a "black-box" approach, where analysis output is accurate but there is no ability to understand the how and why of a particular decision (and therefore control/validate it). An alert may be driven by a number of complex, interlinked variables, but the specific narrative behind it will not be clear. While this is less of an issue for fraud detection, it presents a challenge for AML purposes as it is hard to evaluate and validate from a regulatory scrutiny perspective. Given that regulatory bodies are effectively the client for AML compliance, a lack of regulatory support means that artificial intelligence–based machine learning is really only useful from a supporting rather than frontline perspective.

Oracle's ability to generate and show supporting narrative is an important step in driving regulatory acceptance

The key advance that Oracle is proposing with its new Financial Crime and Compliance Management platform is the ability to provide a "window" to this black box, by providing a way to explain why an alert has been generated within a black-box ML-based model. With this tool, banks will be able to generate the narrative in a pictorial format that shows which variables contributed to a particular decision, and thus banks will be able to explain regulators what the black box is doing.

This is an important step in allowing banks to educate regulators, to show that ML techniques can be used in a meaningful way to support frontline AML monitoring by providing transparency into the logic and workings behind machine-generated models. Obviously, regulatory approval should not be taken for granted, but given that improving detection effectiveness is in all parties' interests (aside from the financial criminals), regulators are likely to be receptive to advances here.

Alongside this, Oracle has made advances in its platform around improving the efficiency of investigations, with its case management tool deployed with graph analytics to correlate alerts from different systems – to look at how tightly these are correlated, as well as relative sequencing over time. This should help identify suspicious patterns (e.g., a sanctions alert with rapid movements of funds), with patterns able to be fed back into alert systems to improve their effectiveness.

With the latest October release, Oracle has developed the platform to allow execution of analysis directly from a financial crime data lake (using in-memory Apache Spark). This is an important development, in that it will allow investigators to analyze far larger data sets (for example, full historical credit card transaction data). It also means institutions can start to move away from having multiple case management systems, with separate corresponding data sets, to work across one data lake, providing both effectiveness and efficiency benefits.

Appendix

Further reading

Countering Financial Crime, IT0059-000086 (January 2017)

Assessing the Role of Big Data in Tackling Financial Crime and Compliance Management, IT0003-000681 (February 2016)

Author

Daniel Mayo, Chief Analyst, Financial Services Technology

daniel.mayo@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo