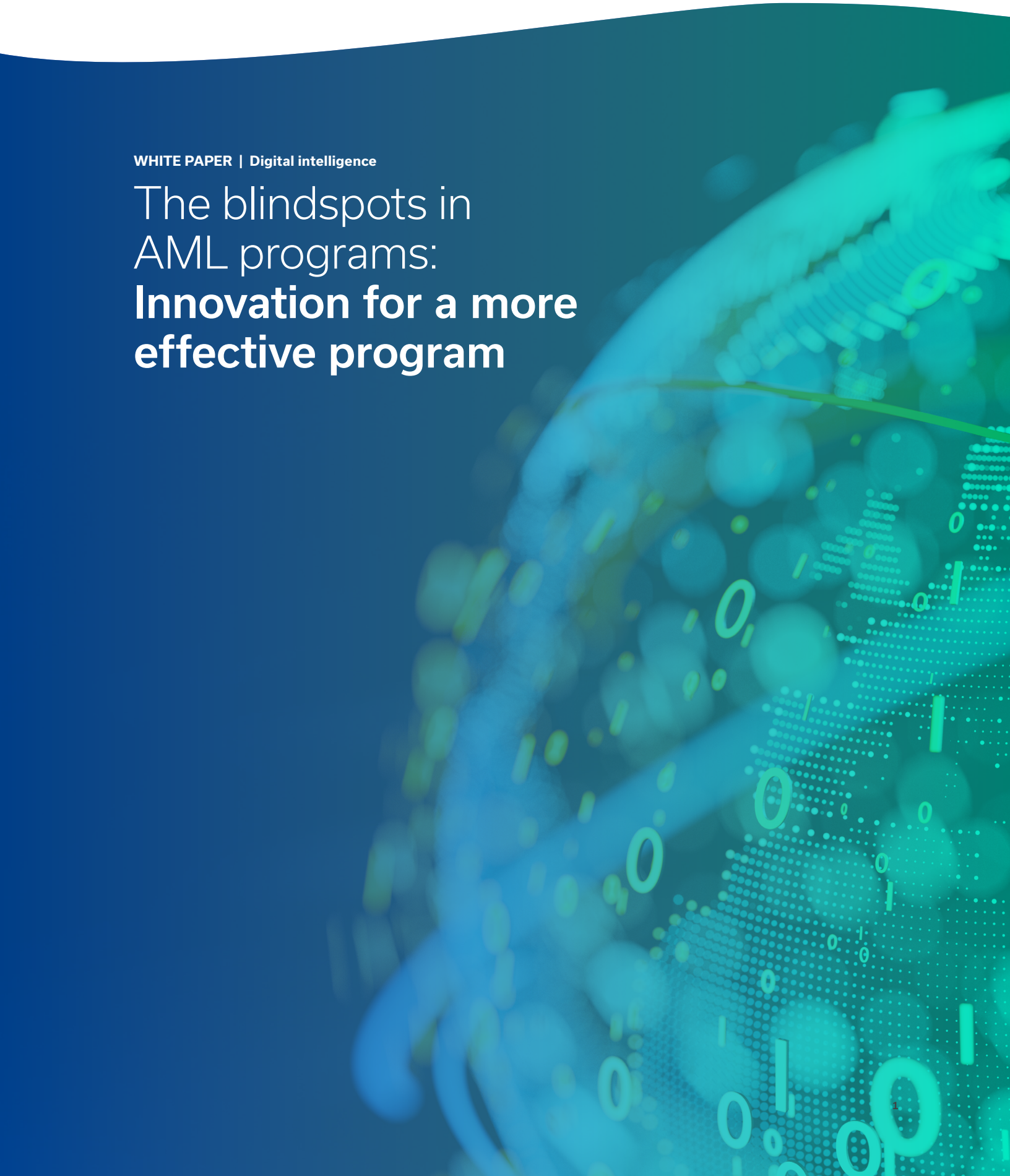
SymphonyAI
SENSA-NETREVEAL

WHITE PAPER | Digital intelligence

The blindspots in AML programs: **Innovation for a more effective program**



Regulatory expectations for financial institutions' (FI) AML programs have pivoted. FIs now must not only achieve technical compliance with rules and regulations but also, and probably more importantly, are expected to effectively mitigate risk.

> ***Ultimately, each FI should be able to demonstrate effectiveness by telling its unique story, based on its risks and corresponding AML/CTF programme. An FI's effectiveness, as it relates to designated priorities or the AML/CTF programme overall, should be measured based on its compliance with law and regulations, how it is designed to provide highly useful information to government authorities in defined priority areas, and how the FI builds and maintains a reasonable and risk-based set of controls to mitigate the risks of the FI being used to facilitate illicit activity."***[1]
>
> **The Wolfsberg Group, June 2021**
> Follow-up on original statement of effectiveness in 2019

The U.S. financial crimes enforcement network (FinCEN) quickly followed The Wolfsberg Group's original statement, releasing in September 2020 its advanced notice of proposed rule-making (ANPRM) on incorporating an "effective and reasonably designed" AML program. The potential regulation would define such a program as one that's informed by the FI's risk assessment and published national priorities, complies with BSA requirements, and reports highly useful information to government authorities. Notably, FinCEN goes on to say, it "does not expect that its strategic AML priorities would capture the universe of all AML priorities, nor would they be intended to serve as the only priorities informing a risk-assessment process."

Criminals continue to become more sophisticated in their schemes, the pace of financial transactions continues to accelerate, and a digital-first world makes the options to conduct nefarious financial activity nearly endless. So, how can FIs be confident their programs are effectively mitigating their risks? Part of the answer lies in the use of technology to effectively identify, understand, and detect their unique risks and exposure. These kinds of solutions can assist in not only identifying current risks but also illuminating emerging and shifting risks, enabling better detection and alert triage, and overall agility through consistent tuning and optimization as risk profiles and typologies change.

[1] The Wolfsberg Group—Demonstrating Effectiveness, The Wolfsberg Group, June 2021, https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Group_Demonstrating_%20Effectiveness_JUN21.pdf

> *So, how can FIs be confident their programs are effectively mitigating their risks? Part of the answer lies in the use of technology to effectively identify, understand, and detect their unique risks and exposure."*

Are your risks really covered?

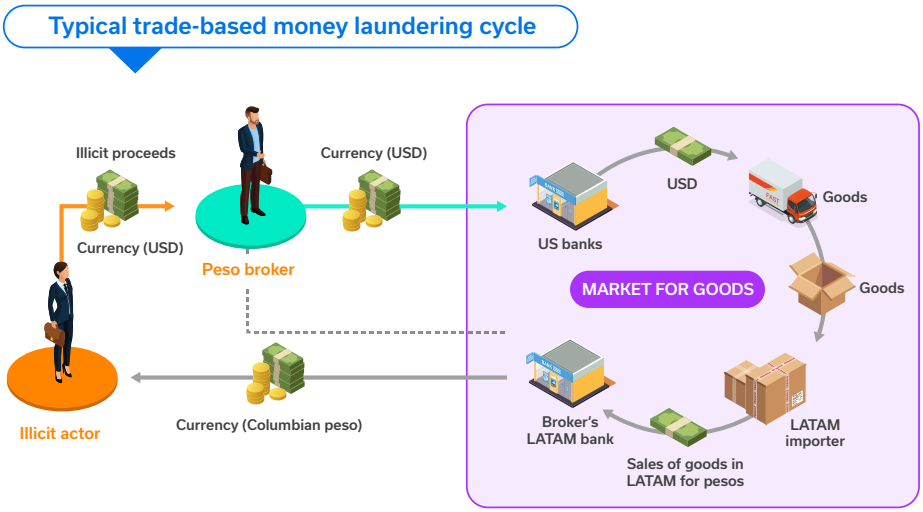
The Wolfsberg Group also in its 2021 Statement said that, when assessing risks, FIs should focus on threats related to defined national or supra-national priorities and employ a more agile, less prescriptive risk assessment process. However, these priorities are often broad categories of threats and aren't always specified to the level of scenarios or red flags. Also, as FinCEN alluded to in its ANPRM, sometimes risks can exist or emerge that aren't specifically listed in such priorities but are related to them. These risks could be a blind spot for an FI and create interpretation and execution challenges for AML programs and, more specifically, transaction monitoring efforts to ensure the FI is effectively implementing risk-based coverage.

Take for example trade-based money laundering (TBML) — goods trading, that is. It has long been a known typology and risk for banks. Much information on TBML has been made available from regulatory and law enforcement agencies and has been covered at conferences and industry events over the years. Moreover, FinCEN in its 2021 AML/CFT National Priorities cited TBML as a method used by drug trafficking organizations to launder money.

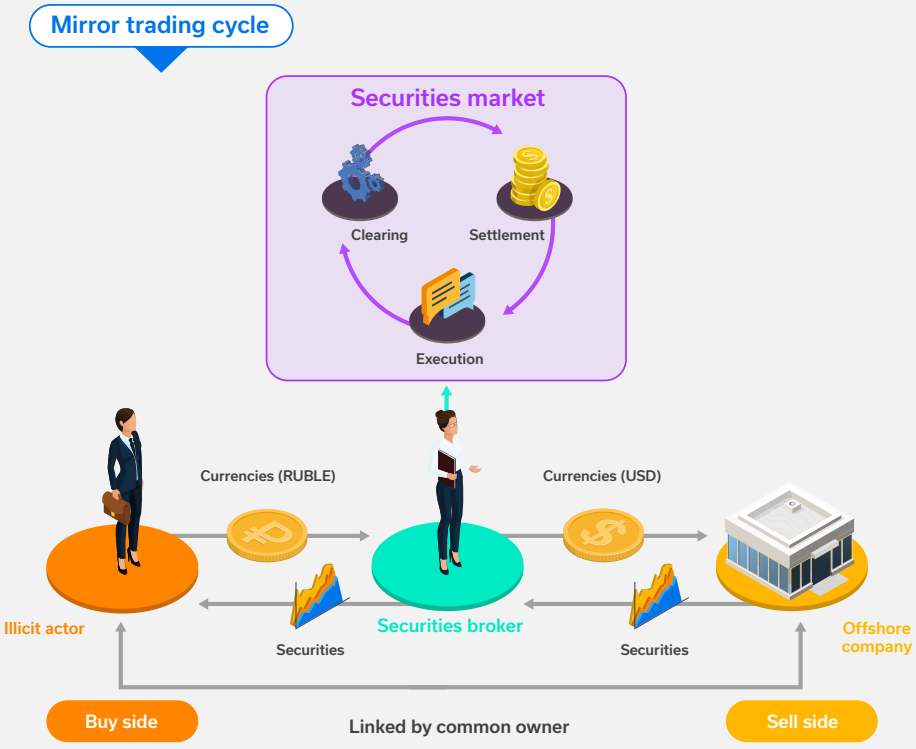
But there are other money laundering schemes using very similar mechanisms as TBML that pose a great risk to FIs and are often missed with traditional rules-based monitoring. Money laundering through securities trading is one that is particularly attractive, offering the opportunity for high-value, fast-paced, difficult-to-detect schemes.

As shown in Figure 1. in a TBML scheme money is laundered through the purchase and sale of licit goods through a "money broker." Likewise, in a "mirror trading" scheme — one that drove more than $600m in fines against Deutsche Bank — a securities broker acts as the gatekeeper, facilitating money laundering through the purchase and sale of securities. In each of these schemes, the gatekeeper provides access to a market — goods and securities — that can be used to launder massive amounts of money.

This is just one example of a potential blind spot and how there might exist multiple money laundering methods related to one or more of these broad national or supranational lists of priorities. There are numerous others and, at this point, FIs would be wise to find opportunities and tools to support them in their journey to improve effectiveness.



Example of a typical trade-based money laundering cycle



Innovative solutions for risk identification and detection

In this new world of AML, with more sophisticated criminals and a faster, digital-first world, technology, including continuous machine learning and simulation, will play a key role in supporting not only proper risk ID and detection, but also risk management and mitigation. But the challenge is not in simply detecting known risks, it's also critical to detect those unknown risks and be agile in order to detect and manage new or changing risks. Innovative technology can help minimize false negatives, improve calibration and tuning of detection models, better prioritize risk, and even guide strategic decisions, including around staffing, products/services, and geographic footprint. It's important, though, for FIs to take care to not only assess and address data requirements and data issues but also policy and governance needs to best position themselves to maximize the benefits of such innovation.

Automated and continuous machine learning:

Full analytics ecosystem that includes data pre-processing and preparation along with self-service modeling techniques, including statistical and supervised and unsupervised machine learning models

Enables feature extraction and evaluation, data visualization, and clustering and segmentation to build predictive models that can then be evaluated to rank performance

Uses detection simulation to individually compare machine learning scenarios to existing rules-based scenarios or compare a current production configuration to a proposed alternate

Prevents model degradation by automating model retraining at scheduled intervals with the latest data ensuring the models are reactive to change and performance accuracy is maintained

Typology simulation:

Simulates financial crime typologies to independently test and visualize the performance of AML detection rules

Supports (1) identification of gaps in detection rules, (2) preparation for regulatory exams, and (3) limits liability for potentially missed risks

In a survey of 153 financial crime professionals conducted by SymphonyAI Sensa-NetReveal, 55 percent were either very interested or extremely interested in such a simulation service

AML transaction monitoring

SymphonyAI Sensa-NetReveal AML transaction monitoring is an end-to-end solution that manages all aspects of anti-money laundering detection, investigation and reporting. Our investigator-centric solution combines human intelligence with machine learning and advanced analytics to drive efficiency and help you prevent more financial crime.

SymphonyAI SENSA-NETREVEAL

- Can be extended to include capabilities for **customer due diligence, watch-list management, sanctioned people and entities, and PEP screening**
- Reduces false positive alerts by **at least 30 per cent**, via machine learning capabilities
- Is trusted by **50 per cent of Europe's largest banks**
- Drives **30-40 per cent faster profiling and detection**

About SymphonyAI Sensa-NetReveal

SymphonyAI Sensa-NetReveal, a division of SymphonyAI, provides leading AI-based financial crime detection software.

Contact us for more information:
netreveal.ai/contact