Suptech applications for anti-money laundering

Workshop on “Big data & Machine Learning Applications for Central Banks”
Rome, 21 October 2019
Marco De Simoni, Expert, UIF, Jermy Prenio and Rodrigo Coelho, Senior Advisors, FSI
The views expressed in this presentation are those of the presenter and do not necessarily reflect those of the FSI or BIS or UIF.
Outline

- Introduction
- AML authorities and mandates
- Data analytics tools used by AML authorities
- Challenges
- Key messages
Introduction

- AML authorities conduct data analysis in order to identify, assess and understand the money laundering and terrorist financing risks in their jurisdictions.
- In conducting data analysis, AML authorities rely on large volumes of data.
- The need to analyse large volumes of data results in certain challenges (collection, quality, completeness).
- Automation of data collection and validation processes addresses some of these challenges.
- AML authorities need to develop data analytics tools in order to more efficiently and effectively analyse information from disparate sources and come up with a complete and coherent picture of AML/CFT risk, either for compliance assessment or detection purposes.
Authorities and mandates

Supervisors

to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing

Financial intelligence Units

the receipt and analysis of: (a) suspicious transaction reports; and (b) other relevant information, and for the dissemination of the results of that analysis

tools that contribute to the detection of suspicious activities

tools that contribute to the compliance assessment of financial institution
Data analytics tools used by AML authorities – AML supervisors

AML supervisors – compliance assessment

- Tools contribute to the compliance assessment of financial institution in different ways
  - Identification of networks to which financial institutions are exposed
  - Evaluation of self assessment by financial institution
  - Risk scoring of supervised entities
  - Assessment of adherence of financial institutions to reporting requirements
Data analytics tools used by AML authorities – AML supervisors

Identification of networks: MAS application of NLP and network analysis to STRs

Narrative portion of STRs

- Focus supervisory attention on financial institutions affected by networks of higher-risk accounts, entities or behaviour
Evaluation of self assessment: DNB application of machine learning and NLP to SIRA reports

- The tool analyses the SIRA reports by answering specific questions
- The tool is trained with the intervention of supervisors who check the answers of the tool
- The objective of the tool is to increase the efficiency in the analysis of numerous and sometimes lengthy documents
The tool applies a heuristic model that uses several risk factors determined by subjecting a significant amount of data to different analyses.

The objective of the tool is to assess the risk profile of each reporting entity in order to help to prioritise onsite supervision examinations.

The output of the model is compared with that of a supervised learning one.
The number of unreported unusual transactions detected will contribute to the assessment of the regulatory compliance of banks and support the prioritisation of onsite inspections.
Data analytics tools used by AML authorities – FIUs

FIUs – detection of suspicious activity

- Tools contribute to the detection of suspicious activities in different ways
  - Detection of networks of entities involved in suspicious activities
  - Assessment of the likelihood of money laundering activity
  - Identification of patterns and trends in criminal activities
Data analytics tools used by AML authorities – FIUs

Detection of networks: UIF application of network analysis and self-organising maps to the Gold database

- The tool uses network analysis to build the networks of actors’ behaviours
- The tool searches the gold transactions database looking for behaviours that are “similar” to fraud schemes that are subject of recent major investigations
- Similarities are identified based on the structure of the network
Data analytics tools used by AML authorities – FIUs

Assessment of the likelihood of money laundering: ROSFIN application of machine learning

Training set: transactions related to money laundering

Test dataset: all transactions

Identification of transactions with characteristics that are similar to those of other transactions related to money laundering

Other application: detection of potentially fictitious companies based on a sample of known shell companies
Data analytics tools used by AML authorities – FIUs

Identification of patterns and trends: FINTRAC application of text mining to STRs

- Similar STRs are aggregated so that trends and patterns can be identified
- Increases in a certain typology may lead to further investigation and also to the development of alerts to reporting entities
Challenges

- Computational capacity
- Data privacy and confidentiality
- Resources (internal or external development, skills)
- Assessment of effectiveness
Key messages

- Important for AML authorities to harness the potential of innovative technology for data analytics
- Exploration or development of advanced data analytics tools could be organised in different ways
- Efficiency gains seem to be the number one benefit of these tools, which could help capacity-constrained authorities
- More international dialogue on this topic would foster peer learning