July 2021

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Brief

Machine Learning: Uniting Banks Against Money Laundering

Money Laundering Series, No. 2

| Craig Nelson | Corie Wieland |
| Lucas Beissner | Tom Westphal |

In recent years, money laundering scandals have disrupted Baltic financial markets and focused attention on financial institutions that have turned a blind eye to high-risk transactions. Fallout from the Danske Bank and Swedbank scandals prompted domestic financial reforms, but Europe-wide laundering networks demand a coordinated multinational effort to detect illicit transactions at their source and prevent further attempts at money laundering. Cross-border and multi-institutional money laundering schemes take advantage of financial authorities' inability to detect complex networks beyond their own borders. Distributed application of a targeted technological approach, such as a federated autonomous deep learning (FADL) algorithm, could provide investigators with greater capcity to deterct suspicious transactions without compromising data security or privacy.

Cross-border and multi-institutional laundering money laundering schemes take advantage of financial authorities' inability to detect complex networks beyond their own borders

Current anti-money laundering (AML) efforts are stymied by high levels of compartmentalisation of sensitive data held by individual banks. All banks keep detailed and confidential records of transactions on behalf of account holders, and compliance officers within each bank's jurisdiction monitor the flow of money for suspicious activity or signs of money laundering.[1] Banks are by nature discreet about account holders' activity and financial patterns. While data privacy is a priority, the compartmentalised activity this leads to prevents regulators from understanding money laundering efforts at an aggregate level. This works to the advantage of people moving illicit funds because they rarely limit their efforts to one bank or even one country. This policy brief proposes a machine-learning approach that allows banks to collaboratively train a shared algorithm to recognise and predict money laundering activity without moving sensitive transaction data into a centralised repository. This approach will enable compliance officers to detect money laundering schemes with greater efficiency without compromising data security or privacy.

A Question of Capacity

The past two decades demonstrated that individual banks and Financial Intelligence Units (FIUs)—state-level monitoring agencies that identify illegal financial activity—lack the capacity to prevent large-scale money laundering operations across the European Union's financial system. FIUs rely on the banks in their countries to detect and report money laundering activity. However, banks value discretion and are hesitant to share information with each other, so individual banks can only confront money laundering within their own fragmented view of the multinational banking system. An FADL application to AML efforts is in the public interest because it addresses compartmentalisation at the FIU and banking levels.

The scandals surrounding Danske Bank and Swedbank in Estonia hinged on a chain of shell companies that was too extensive and complex for compliance officers to fully appreciate.[2] The files leaked from the US Department of Treasury in September 2020 indicate that because banks are legally responsible for detecting and reporting any suspicious activity from account holders, they are overly cautious in identifying suspicious activity and overwhelm FIUs with more information than they can reasonably staff.[3]

In July 2020, the European Commission's Action Plan for a comprehensive policy against money laundering armed the European Banking Authority (EBA) with more authority over EU-based banks and directed the EBA to establish a database that would allow FIUs to develop and share risk assessments of banks from across the EU's jurisdiction.[4] The Action Plan directives are positive steps, but they do not give banks or FIUs the capacity necessary to keep pace with money launderers who act with an understanding of the entire banking system. The proposal set out in this policy brief would provide that capacity and address the conditions that required the Action Plan to begin with.

The proposed multilateral, multi-institutional algorithm would build upon previous efforts to aggregate and learn from banking data for AML purposes. In July 2015, Articles 53 and 56 of the EU's fourth Anti-Money Laundering Directive required member-state FIUs to actively share data with each other and work together to analyse cross-border money laundering cases.[5] The European FIU Network (FIU.net) connected national-level FIUs through a decentralised database that allowed analysts to search anonymised versions of suspicious transaction reports.[6] FIU.net used an algorithm to match search queries to the characteristics of irreversibly anonymised data supplied by participating FIUs.[7] However, FIU.net's oversight by Europol, a law enforcement agency, prompted a ruling under the General Data Protection Regulation (GDPR) in 2019 that resulted in the network's suspension. The plan for its return is still in progress.[8]

A Federated Approach

Banks already collect and analyse customers' transaction data to identify suspicious activity, and they already share their findings with national authorities without alerting account holders. Banks currently do this with help from rules-based software that looks for pre-programmed conditions in transaction data. But as large-scale money laundering scandals have shown, this approach is problematic, because that software must be manually calibrated to stay abreast of current money laundering trends, and each bank's proprietary system does not incorporate broader knowledge from other banks. Furthermore, banks in Europe and elsewhere do not typically collaborate or share sensitive data with each other. As long as this is the case, anti-money laundering efforts in the EU will never amount to anything greater than the individual efforts of banks in its member states.

What is missing is a way for banks to work together without jeopardising the information that makes them competitive against each other. If the EBA provided its banks with a machine learning algorithm that enabled large-scale pattern detection on internal data, it would grant banks the benefit of collective insight without jeopardising data security, privacy, or proprietary information.

Machine learning algorithms grow stronger with higher quality and quantity of data. To ensure an effective FADL model, the EBA should account for variance in regional and consumer patterns by training the algorithm in institutions in as many areas and with as many unique services as possible. The EBA should also promote full participation to limit the possibility of participating banks only partially applying the algorithm to a pre-selected subset of data, which would be counterproductive to the AML effort.

> *What is missing is a way for banks to work together without jeopardising the information that makes them competitive against each other*

In a centralised model, the security risks associated with moving data from participating banks into a centralised location include the physical and digital security of the database as well as privacy and due process concerns related to access. It is possible to mitigate those risks through measures like cryptography or differential privacy, but a better idea is never to move sensitive data from their original location. In federated learning, an algorithm moves to various data sources for localised training, adjusts parameters to reflect aggregate values, and is redistributed to institutions to detect both large-scale and localised money laundering schemes. Once redistributed, the algorithm continues to train on local data in real time and grants participating banks faster detection of evolving schemes (see Figure 1).

> *The EBA already oversees current EU-wide AML efforts under legislative authority and is a natural entity to manage data processing and protection*

Because participating banks would not have to move their data, this method seems most conducive to the banking system's heightened requirement for data security and privacy. If the EU's large banks collaborated to train a learning algorithm from their own transaction data, they could each employ that algorithm with the benefit of collective insight. They would possess a collaborative tool that would be regionally tailored and would employ an aggregate-level understanding of the most current money laundering trends.

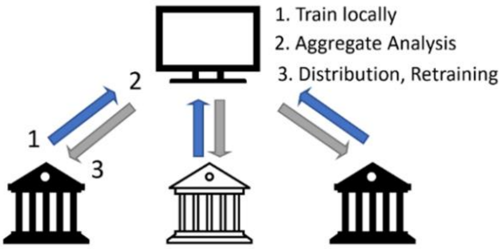

Figure 1. FADL Application to AML

Machine Learning and the GDPR

The EU guards its citizens' data and privacy with the General Data Protection Regulation (GDPR), and it is important to address how this proposal would comply. Previous decentralised database efforts failed in part due to GDPR violations. To ensure full compliance and data privacy protection, development of an FADL algorithm should consider four elements outlined by the GDPR: 1) the identification of a Controller, responsible for overall data processing and protection; 2) assignment of a Processor that handles and protects data according to the Controller's specifications; 3) acknowledgement of the Data Subject's rights to control storage of and access to sensitive information; and 4) the designation of a Supervisory Authority to ensure full GDPR compliance at all stages.[9]

The EBA already oversees current EU-wide AML efforts under legislative authority and is a natural entity to manage data processing and protection as Controller.[10] A Software-as-a-Service provider could act as Processor by establishing a private cloud-based computing environment for algorithm training and following suggestions from the European Union Agency for Cybersecurity to ensure cloud-based security.[11] Participating banks should inform Data Subjects of their rights to opt out, access their data, know where their data are stored and processed, and to request erasure.[12] And at the supranational level, the European Data Protection Supervisor, a public entity that enforces GDPR compliance, is most appropriate as a Supervisory Authority.

Looking Ahead

The ultimate outcome for an FADL model is for European banks and FIUs to augment their individual AML efforts with a broader understanding of illicit trends and patterns across the EU banking system at large. Supplying banks with a robustly trained machine learning algorithm would be a wide-ranging and uniformly applied change that would equip compliance officers with far greater ability than they could ever achieve on their own. With appropriate direction, the EBA can develop and deploy a privacy-minded algorithm that protects the rights of data subjects while enforcing effective AML mechanisms throughout the European banking system.

Endnotes

[1] Simon Bowers, Karrie Kehoe, and Holger Roonemaa, "Inside Scandal-Rocked Danske Estonia and the Shell-Company 'Factories' that Served it," International Consortium of Investigative Journalists, 21 September 2020.

[2] Michael Lund, Simone Bendtsen, and Eva Jung, "Report: Russia Laundered Millions via Danske Bank Estonia," Organized Crime and Corruption Reporting Project, 26 February 2018.

[3] Matthew Collin, "What the FinCEN Leaks Reveal About the Ongoing War on Dirty Money," Brookings, 25 September 2020.

[4] European Union, European Commission, "Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing," 7 May 2020.

[5] European Union, European Parliament and the Council of the European Union, "Directive (EU) 2015/849 of the European Parliament and of the Council," Official Journal of the European Union, 20 May 2015.

[6] Clare Ellis, and Inês de Oliveira, "Tackling Money Laundering Towards a New Model for Information Sharing," Royal United Services Institute for Defence and Security Studies, Occasional Paper, September 2015, 15.

[7] Udo Kroon, "Ma^{3}tch: Privacy and Knowledge: 'Dynamic networked collective intelligence'," 2013 IEEE International Conference on Big Data, September 2013, 23-31.

[8] The issue was not about the exchange of anonymised data, but rather the nature of the organisation controlling FIU.net. As a law enforcement agency, Europol cannot retain the personal data of EU citizens who are not investigation suspects, and persons listed on suspicious transaction reports are not necessarily suspects. In its July 2020 Action Plan, the EU Commission announced that it planned to administer FIU.net until they arrange something more permanent.

[9] Dimitra Georgiou and Costas Lambrinoudakis, "Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)", Information 11, no. 12 (December 2020), 5.

[10] European Banking Authority, "Risk Assessment Under Article 9a of the EBA Regulation," 16 December 2020.

[11] Dimitra Liveri, Athanasios Drougkas, and Antigone Zisi, *Cloud Security for Healthcare Services*, (Athens: European Union Agency for Cybersecurity, 2021), 29-38.

[12] Georgiou and Lambrinoudakis, "Compatibility of a Security Policy," 5.

About the Authors

Craig Nelson, Corie Wieland, Lucas Beissner, and Tom Westphal

Craig Nelson, Corie Wieland, Lucas Beissner, and Tom Westphal are graduate students in the Freeman-Spogli Institute's Master's in International Policy programme at Stanford University. This brief series is part of the final capstone project for their master's programme, intended to address issues related to deterring Russian aggression in northeast Europe.

Disclaimer: The views and opinions contained in this paper are solely of its author(s) and do not necessarily represent the official position of the International Centre for Defence and Security or any other organisation.

ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076