INSTITUTE *of* INTERNATIONAL FINANCE

October 2018

Machine Learning in Anti-Money Laundering – Summary Report

This public version of the report is a short-form summary, highlighting the key findings. The full detailed version is restricted to the regulatory community and the 59 institutions that participated in the IIF survey.[1]

1. Introduction

The prevention of money laundering and terrorist financing is a key topic in the entire financial sector. For years, its importance in the eyes of financial institutions of all sizes and business models has grown exponentially, along with the focus of lawmakers, regulators and supervisors. Preventing the financial system from being misused to launder illicit funds or to fund terrorist attacks is a key feature in the global effort to reduce the devastating effects of crime and terrorism.

Despite these efforts, the level of undetected illicit funds remains too high. Financial institutions are increasingly turning to new technologies to address the issue, among them machine learning.

Machine learning techniques hold great promise in addressing some of the challenges financial institutions are grappling with. They can be used to increase the efficiency of measures in the various elements of the AML framework, for example to reduce false positive and improve the effectiveness of transaction monitoring.

For this study, the IIF surveyed 59 financial institutions (FIs) on their application of machine learning techniques in combatting money laundering. These institutions comprised 54 banks and 5 insurance companies, representing firms from all continents and across a diverse range of business models and firm sizes. This followed an earlier IIF study on the application of Machine Learning in Credit Risk.[2]

2. Application of Machine Learning in AML

For the purpose of this report, we chose a similar definition of machine learning as in our previous initiative on its application in credit risk. Advanced analytical techniques showing the following attributes qualify as machine learning techniques in this context:

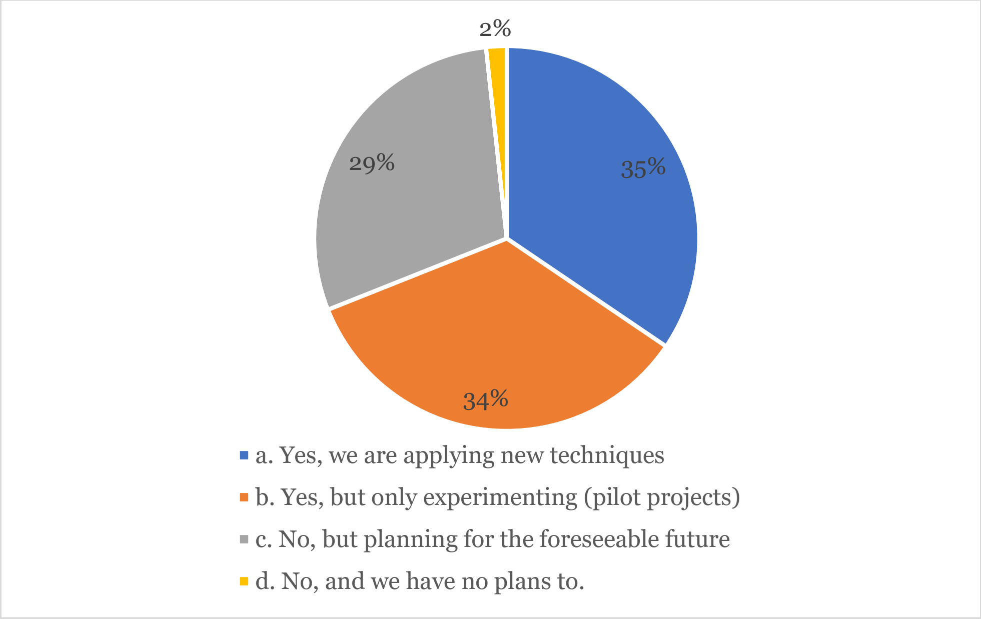
1. The use of cross-validation to model relationships in the data;
2. A primary goal of out-of-sample predictive performance using regularization;
3. A significant degree of automation in the model development process;
4. Applicability to very large volumes of data, in some cases including unstructured data sources.

[1] The detailed report is available to employees of regulatory agencies and participant firms on request.

[2] The IIF's Summary Report Machine Learning in Credit Risk can be found on the IIF website at https://www.iif.com/publication/regulatory-report/machine-learning-credit-risk

The majority of financial institutions surveyed already use (35% of participants) or experiment (34% of participants) with machine learning techniques. Another 29% indicated that they are planning on applying new analytical techniques in the foreseeable future. However, the industry is still cautious in its application, as shown in the use cases in Section 3.

Figure 1: Do you apply new analytical techniques and technologies in your AML-related analysis (58 firms)



3. Use Cases and Benefits for Machine Learning in AML

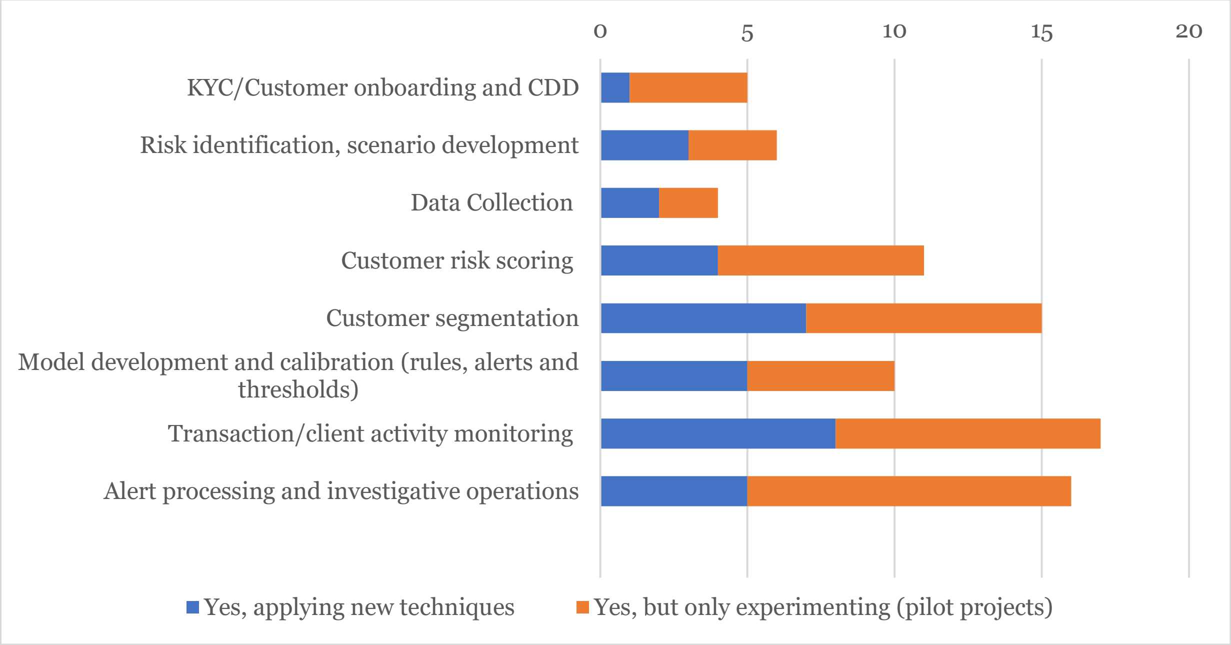
3.1. Use Cases

Machine learning is not set to fundamentally change the approach to AML but rather to enhance and rethink processes for existing elements of the framework, such as transaction monitoring, risk assessments and Know-Your-Customer (KYC). Within these elements however, the effects could be profound.

The various stages of transaction monitoring are the main focus area for machine learning, identified by 33 of the 59 participants. Use cases range from applying enhanced analytics as an additional filter to the existing monitoring systems to reduce false positive numbers, to combining traditional approaches with graph theory and supervised machine learning to conduct the monitoring itself. The most experimental use cases look at a possible paradigm shift towards a holistic approach to monitoring, best described as customer behavior monitoring. The current focus on transactions is expanded by leveraging information from KYC files, other business conducted with the institution and information from external sources to identify potentially suspicious activity (or prevent unnecessary alerts in the first place).

Common to these use cases is that the human element of AML is preserved. The consistent aim is to free the resources of a firm's analysts to focus on higher risk cases, thus where they are most valuable. Financial institutions are not currently looking to automate the decision-making process, but to support their analysts with increasingly powerful technology and automating process steps that keep them from focusing on the relevant risks.

Figure 2: Stages in the AML process where FIs are applying or experimenting with new analytical techniques

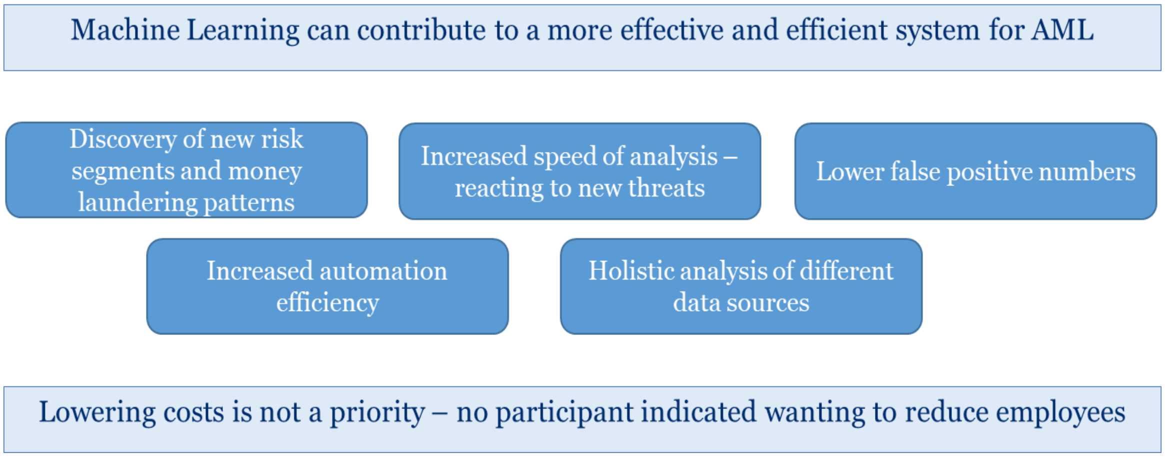


Firms also work on customer segmentation and risk modelling, building models that consider a variety of risk factors and allow more flexibility by overcoming data gaps (for example using graph theory), ultimately resulting in a more precise risk assessment of customers and across the institution. The lowest number of projects are run to improve KYC processes, looking at overcoming data gaps and processing unstructured customer data. In this context, we have identified a strong use of Natural Language Processing to collect insights from adverse media / negative news sources. These projects may often be at an experimental stage, but it highlights the importance of building consistent processes in this respect.

3.2. Benefits

While participants are evenly split between actively applying and experimenting with machine learning, how advanced the industry is varies depending on the technique. Our analysis has shown that the expected benefits were indeed realized by those who already apply machine learning. With more advancement in the field in the future, we expect further benefits to arise.

Figure 3: Benefits of Machine Learning in AML



Machine Learning can contribute to a more effective and efficient system for AML

Discovery of new risk segments and money laundering patterns

Increased speed of analysis – reacting to new threats

Lower false positive numbers

Increased automation efficiency

Holistic analysis of different data sources

Lowering costs is not a priority – no participant indicated wanting to reduce employees

The most prominent benefit is increased speed and/or automation of analysis that allows the AML process to respond to the latest development in money laundering methods. This increase in automation and speed of key process steps will be beneficial to all other process steps built around them.

We have also found that the expected ability to identify completely new risk segments and patterns that might point to money laundering or other types of illicit activity has indeed been realized. Institutions clearly leverage the inherent capabilities of enhanced analytics to strengthen their defense systems. This new knowledge can be used to build new typologies in existing risk models both for risk assessment and monitoring purposes. We have also observed significant advancements in customer segmentation capabilities. By analyzing an entire customer base for similarities using an unsupervised machine learning approach, firms are able to identify outliers and investigate if further action is warranted, thus gaining an even more precise view of the risk they might be exposed to.

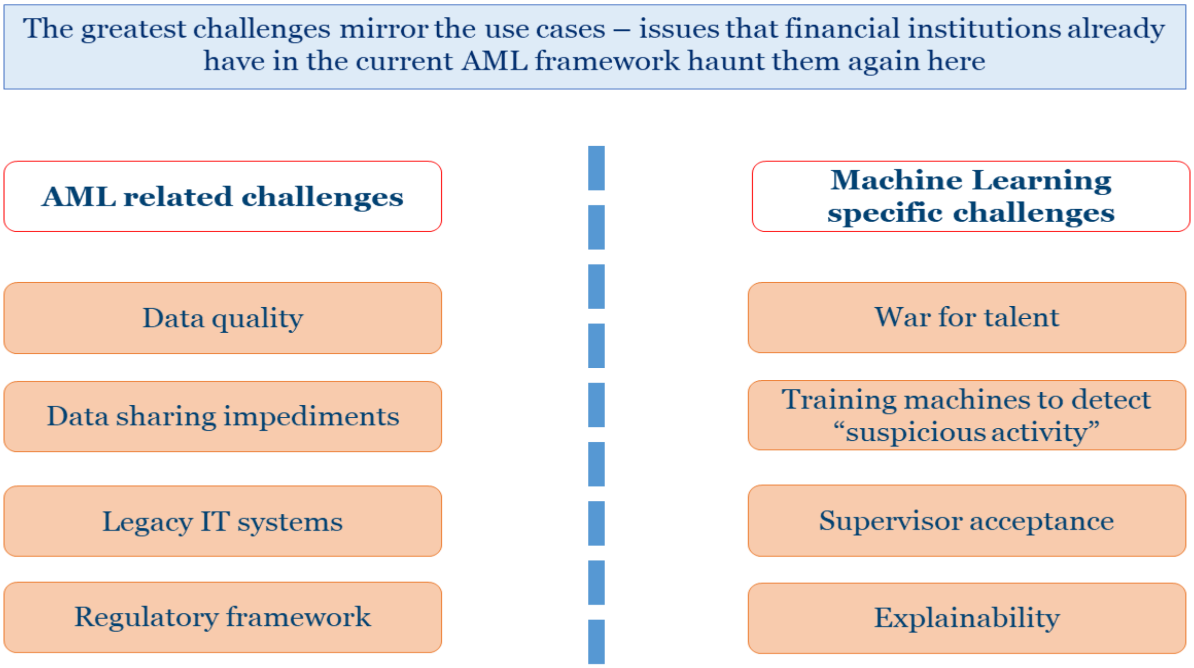
Unsurprisingly, firms have also reported a reduction of false positive rates, i.e. alerts that are generated but do not present any risk. Some of these reductions were considerable. We have also had reports of firms having generated alerts that would have remained undetected under the traditional rules-based approach, as well as an increase of alerts that warrant investigating (even if they turn out not to indicate illicit activity). An increase in the quality of generated alerts that leverages a higher level of automation in process steps does indeed allow to focus the human experts on the most relevant cases. This is increased where firms have indicated that they have been able to process information from various data sources, showing the potential of a holistic analysis.

It should be mentioned that while a reduction in false positives might occur when the monitoring itself is conducted using machine learning techniques, it is unclear if there would be a heavy increase in conversion of alerts to STRs/SARs if rolled out at scale. By leveraging more data sources and using a broader view, more unusual behavior would be identified, but not all unusual behavior is systematically an indication of money-laundering. A higher quality of alerts however could lead to more (precise) reports to the FIUs.

4. Challenges and Recommendations

An interesting observation was made in terms of the challenges encountered. Some of the issues known as barriers to a stronger AML framework come back to haunt the industry in the application of machine learning techniques. At the same time, machine learning itself and its application present their very own challenges that need to be overcome.

Figure 4: Main challenges of applying Machine Learning in AML


The greatest challenges mirror the use cases – issues that financial institutions already have in the current AML framework haunt them again here
AML related challenges
Machine Learning specific challenges
Data quality
Data sharing impediments
Legacy IT systems
Regulatory framework
War for talent
Training machines to detect "suspicious activity"
Supervisor acceptance
Explainability

4.1. Regulatory

Some uncertainty remains regarding the support of regulators for this technology as part of an adequate risk mitigation framework. The IIF recommends a stronger statement of support for the application of new technologies in the prevention of money laundering and financial crime, as well as a cooperative approach between public and private sector to determine best practices for the methodology in this context. Balancing financial crime prevention measures and privacy rules can also be tricky. We recommend clarifying how institutions can best navigate both frameworks.

Regulators should also be mindful to prevent regulatory fragmentation. If financial institutions faced a more aligned global framework, they could leverage the enhanced capabilities of machine learning techniques more effectively, and do not need to be tailored to the specific requirements of various jurisdictions. A stronger international cooperation is needed to address the evolution of technology for payment systems and standards and how these should be treated from an AML perspective.

One participating institution insightfully identified that "KYC is an enabler for machine learning". High quality data (including KYC data) is key to an effective application of machine learning. We therefore reiterate the importance of supporting every initiative related to the digitization of identity information in a consistent and portable way.

4.2. Explainability

The primary goal of machine learning is to get good out of sample predictions, and the use of regularization to penalize excessive complexity. Many experts agree that there is a trade-off between the predictive accuracy of a model, and model interpretability. Put simply, a linear regression is typically easier to interpret but does not have sufficient predictive power. Whereas in the other extreme, a powerful neural net with millions of parameters can give better predictions but is jarring to interpret.

The challenges around explainability of risk models and algorithms based on machine learning techniques cannot be solved through one recommendation. A more sensible approach is to determine a number of contributing factors, including:

- Acknowledgment by regulators and industry that the need for explainability depends on the use case, e.g. only where decisions are automated;
- Cooperation within the financial industry and between the public and private sectors on determining the expectations to an explanation;
- Devising a transitional model in cooperation between the public and private sectors for the implementation of machine learning based models, for example in transaction monitoring (gradual transfer of transactions to new monitoring approaches, common review between firms and regulator/supervisor after each phase);
- Assessing (in cooperation between public and private sectors) which alternatives can be explored that would balance a loss of explainability in case this is necessary (e.g. demonstration of effectiveness of results and/or methodology in building the model).

The IIF will shortly be publishing a white paper on machine learning explainability that builds on our earlier credit risk report, and will welcome further engagement between the private and public sectors on this topic.

4.3. Data sharing frameworks

Perhaps the biggest challenge however relates to data. Financial institutions are aware that they could potentially identify risks more precisely through the large amounts of information they hold. It is understood that customer financial data must be kept secure and private, which is a responsibility that financial institutions take seriously and have shown to uphold.[3]

However, data sharing restrictions (within financial groups, between financial institutions and between governments and firms) prevent firms from aggregating information and monitoring processes to have a comprehensive

[3] See also the IIF paper Safeguarding Customer Data in the Financial Sector, July 2018, to be found at https://www.iif.com/publication/regulatory-report/safeguarding-customer-data-financial-sector

view of customers and risks. These restrictions are one of the most important barriers to a more effective AML/CFT framework and it is crucial that these are reevaluated.

Despite the welcome steps taken by the FATF in the recent months,[4] further efforts are needed to address challenges to operative sharing of AML/CFT information – including mitigating such issues as inconsistent legal frameworks for data protection, management of SAR-type information, privacy, and bank secrecy - across different jurisdictions. Restrictions implemented at the domestic level, which lead to regulatory fragmentation and weaken an effective AML risk mitigation must be overcome.

In practice, it should be clearly stated in the applicable AML/CFT laws that it is permissible to share and process the relevant information (i.e. KYC information and monitoring results) among members of the same banking or insurance group to prevent financial crime, even if there is no suspicion about a customer. The same must be possible for a central generation of data features based on accessible data sources and processing such shared information, as well as the flow of alerts and other investigations.

How information can be shared between different financial institutions to prevent financial crime needs to be harmonized. It needs to be possible for a firm that has knowledge or is investigating concerns about a customer to warn another where appropriate. This could be inferred by an incoming transaction. We also encourage all national supervisors where such rules have already been implemented to promote and support these possibilities more openly. The financial sector would benefit from more clarity that institutions sharing information among them in this context will be accepted.

The cooperation between the public sector and the financial sector should be revised as well. The "feedback loop" between financial institutions filing STRs/SARs and their outcome should be strengthened. The mechanisms set out in the recently revised FATF Recommendation 2 should be implemented on a national level as well, accompanying a revised framework for information sharing for the private sector and a more comprehensive framework for information flows between the private and the public sector.[5]

The IIF also highlights the importance of a consistent and coordinated approach to allowing these data sharing flows to prevent ambiguities and regulatory fragmentation as much as possible.

While these issues arise, the cooperation between public and private sector in exploring these technologies is encouraging so far. Regulators and firms seem to cooperate in many cases to gain more comfort with this technology and assess common benefits. This welcome development should be pursued further, and can be the basis to address the highlighted challenge on a cooperative basis between public and private sector.

4.4. Access to registry data– needs-based approach

The IIF suggests to allow financial institutions more access to data that the public sector holds, such as databases from tax authorities, registries and law enforcement. Based on the concept of the beneficial owner registries (introduced by the 4th EU AML Directive in 2017), we propose a needs-based approach to government held information, including tax information, law enforcement databases and other registries. Financial institutions would need to demonstrate to fulfil their obligations to prevent money laundering and countering of terrorism

[4] The Financial Action Task Force (FATF) Guidance, Private Sector Information Sharing November 2017

[5] FATF, *Outcomes FATF Plenary*, 21-23 February 2018

financing to access information. This approach would pay tribute to the fact that both ends of the data transfer pursue the same goal, i.e. to prevent the misuse of the financial system for criminal activity.

The tax-related information in particular is extremely valuable, as it can give insight into a (legal or natural) person's residency, occupation and declared income. It can be compared to the information held at a financial institution, which can react in cases where there are doubts about its accuracy.

4.5. Recommendations for industry – Investments in IT and data integrity

Some of the main challenges such as data quality and enhancing the IT infrastructure are for financial institutions to address, and there is strong evidence that this is occurring.

The modernization of IT systems, as well as refreshing and streamlining the content of the existing databases is becoming more and more of a priority. This encouraging development should be pursued and move even further up on the list of priorities for financial institutions.

Failing to do so could have severe consequences for the financial sector. Outdated, incompatible or overly complicated IT system landscapes make institutions more vulnerable to external cyber-attacks. Financial institutions are conscious of these risks and are taking action. They are already dedicating considerable investments in upgrading and maintaining their IT systems to fully benefit from evolving technologies. This will need to continue in order to maintain such a capability.

A modernization of data sets and a higher degree of data integrity is also an important measure to prepare for the increasingly data-focused economy. Beyond historical data and records, ensuring strong data integrity in future datasets is paramount. The latter will benefit from the investments made into the IT infrastructure.

Low quality data is a major source of risk for financial institutions that needs to be addressed. The added side-effect is that a consistently high data quality will also lead to more efficient internal processes, including in investigations departments. It will also lead to a better training capability when developing risk models using machine learning techniques. Using new analytical techniques such as machine learning needs high-quality data, as well as updated IT capabilities and infrastructure.

One key step of the data mining processes and of using techniques such as machine learning is "exploring and cleaning the data, thus integrating typical "data mining processes" into a firms' business. A considerable number of firms are looking at the appropriate use of cloud computing and centralized data aggregation to build an effective (and efficient) basis to leverage these technologies. Especially for larger, multinational financial institutions, these potential moves are becoming more and more important, reaffirming the importance of overcoming barriers to data sharing.

5. Conclusion

The application of machine learning and artificial intelligence is spreading in the financial industry and increasingly includes the RegTech area as well. Particularly for the prevention of financial crime, we are seeing a growing number of institutions exploring the capabilities of this technology. We fully expect this trend to continue, with more firms reviewing their processes and launching projects in this space. This will add to the already considerable number of firms involved in these projects, bringing them to maturity and potentially identifying further areas in which to apply these techniques.

The emergence and development of enhanced analytical capabilities in general and of machine learning techniques in particular will not fundamentally change the way financial institutions tackle the fight against money laundering and terrorist financing. The existing pillars of the framework will continue to dictate which elements must be covered to build a resilient defense system. Rather, machine learning presents an opportunity to significantly enhance the effectiveness and efficiency of the existing measures. There is strong evidence that it this is the case, as the reduction in false positive rates and already better transaction monitoring results have shown. The same is true for every new pattern of suspicious activity or unusual behavior that is identified through these means and was unknown before. Greater automation also grants more flexibility in how these measures are applied and to connect these much more thoroughly than before, such as feeding monitoring results into risk ratings automatically. This allows financial institutions to build a stronger safeguarding framework without putting unnecessary strain on staff resources.

However, some major work needs to be done on all fronts to enable these results. As we have shown, the major challenges to overcome are not overly different from the ones the industry faces already today.

Financial institutions and regulators must work together to devise a harmonized, consistent and sustainable framework around the usage of data. While existing safeguards must not be loosened to the detriment of the protection of the customer or market integrity, financial institutions have demonstrated their expertise at implementing and following these rules. This should make it possible to leverage the existing data in financial groups by allowing them to share it, apply a holistic view of the customer and identify illicit activity. Illicit activity which does not stop at borders can only be tackled efficiently if the information necessary to stop it can be aggregated across these borders. At the same time, a broader exchange of information between the public and the private sector, as well as building partnerships for AML purposes must be a priority.

These partnerships should also extend to exploring the capabilities of technology, ultimately developing the framework together in which these techniques can be applied, and the algorithms used can be explained. Some requirements that have been developed in a time where they were the only way to meet the goals of the overarching AML and CFT framework should be revisited.

The IIF applauds the significant progress that has already been made, and encourages all actors to continue on this path, and to resolve the key issues outlined in this report. When this groundwork is completed, a real and tangible benefit from these techniques that goes beyond the value for a single organization and towards a stronger and healthier financial system could be the result.

Lead Authors:

Adrien Delle-Case
Policy Advisor
adellecase@iif.com

Natalia Bailey
Associate Policy Advisor
nbailey@iif.com

Contributors:

Brad Carr
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

Matthew Ekberg
Senior Policy Advisor
mekberg@iif.com

iif.com © Copyright 2018. The Institute of International Finance, Inc. All rights reserved.