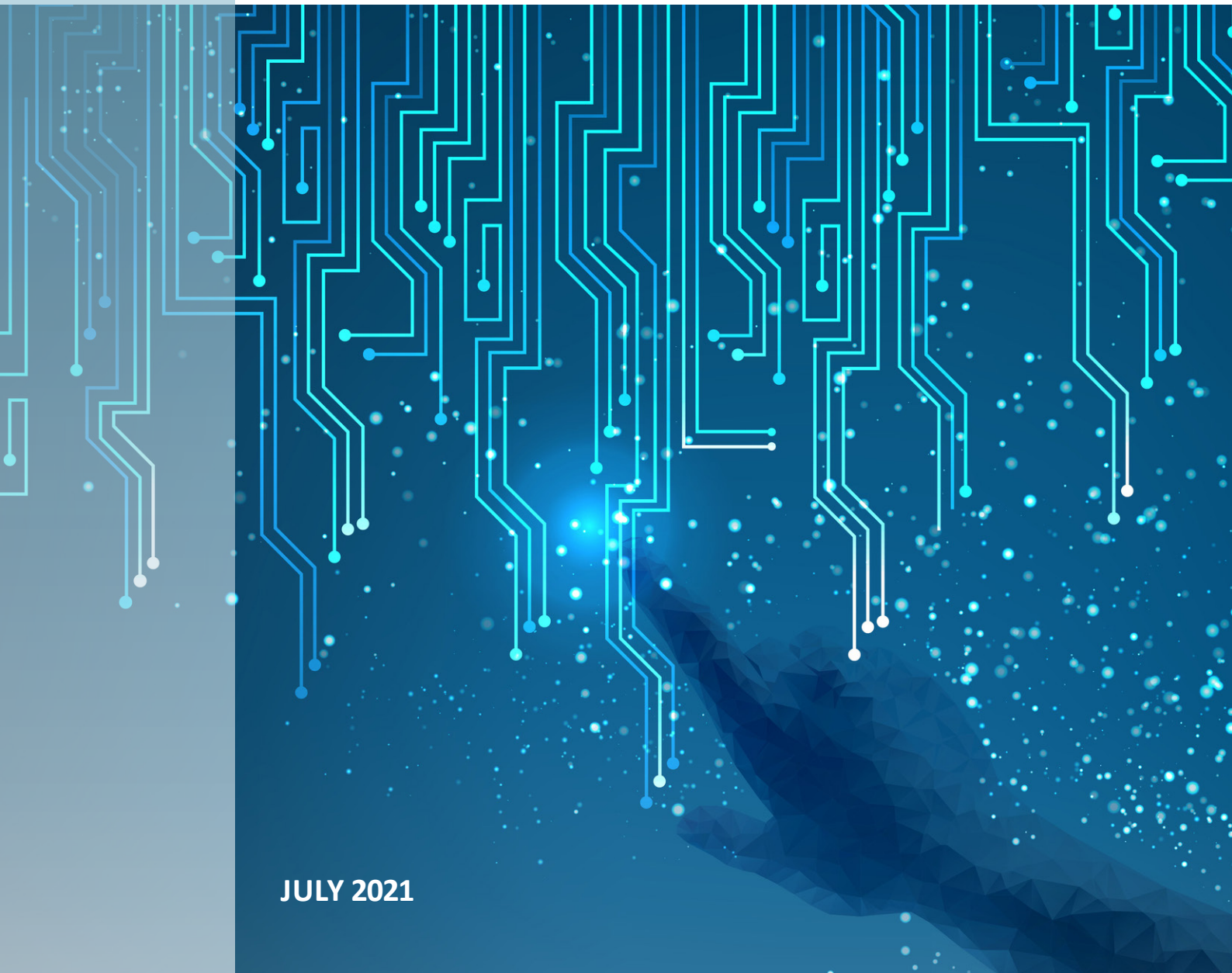
FATF

OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT



JULY 2021

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2021), *Opportunities and Challenges of New Technologies for AML/CFT,* FATF, Paris, France, https://www.fatf-gafi.org/publications/ fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html

Photocredits coverphoto: Gettyimages

Acknowledgements

The FATF would like to thank public and private sector stakeholders—including technology developers, financial institutions and other experts—for providing valuable input, case studies and feedback to this report.

The work of this report was led by the FATF Secretariat (Inês Oliveira), with significant input provided by a Group of Experts from the following FATF delegations: Canada, Denmark, European Commission, Egypt, Germany, Israel, Italy, Japan, Malaysia, the Russian Federation, Singapore, United Kingdom, the United States, as well as Europol and the Secretariat to the Eurasian Group (EAG) on Combating Money Laundering and Financing of Terrorism.

Table of contents

Acronyms 3

Executive Summary 4

1. Introduction 6

1.1. FATF Commitment to Responsible Innovation and Digital Transformation 7
1.2. Scope and Methodology 9

2. New Technologies for AML/CFT: towards a more effective implementation of FATF Standards 11

2.1. Implementing the risk-based approach 13
2.2. Financial Inclusion 15

3. The Opportunities of New Technologies for AML/CFT 19

3.1. Artificial Intelligence (AI) 21
3.2. Natural Language Processing and soft computing techniques 23
3.3. Distributed Ledger Technology 26
3.4. Digital Solutions for Customer Due Diligence 27
3.5. Application Programming Interfaces (APIs) 31

4. The Challenges of Implementation of New Technologies for AML/CFT 36

4.1. Regulatory challenges 36
4.2. Operational Challenges 40
4.3. Unintended Consequences and Potential for Abuse 42
4.4. Assessing AML/CFT effectiveness of technology solutions and how to address residual risks 44

5. Creating an enabling environment for the use of new technologies in AML/CFT 46

5.1. Technologically-Active Supervisors 48
5.2. Concluding remarks 53

Annexes 54

Annex A: Glossary 55

Annex B: Suggested Actions to Support the Use of Technology in AML/CFT 60

Annex C: Case Studies 62

Annex D: Additional RegTech case studies for the uses of new technologies for AML/CFT 67

References 70

Acronyms

AI	Artificial intelligence
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
API	Application Programming Interface
CDD	Customer Due Diligence
DL	Deep Learning
DLT	Distributed Ledger Technology
DNFBP	Designated Non-financial Business and Profession
FATF	Financial Action Task Force
MER	Mutual Evaluation Report
ML/TF	Money Laundering/Terrorist Financing
MVTS	Money or Value Transfer Service
NLP	Natural Language Processing
NRA	National Risk Assessment
PEP	Politically Exposed Person
PSCF	Private Sector Consultative Forums
SSB	Standard Setting Body
VASP	Virtual Asset Service Provider

Executive Summary

1. New technologies have the potential to make anti-money laundering (AML) and counter terrorist financing measures (CFT) faster, cheaper and more effective. They can improve the implementation of FATF Standards to advance global AML/CFT efforts, ensure financial inclusion and avoid unintended consequences such as financial exclusion.

2. As the global AML/CFT standard setter, the FATF is strongly committed to keeping abreast of innovative technologies and business models in the financial sector and to ensuring that the global standards remain up-to-date and can enable "smart" financial sector regulation that both addresses risks and promotes responsible innovation. Accordingly, the FATF reviewed the opportunities and challenges of new technologies for AML/CFT to raise awareness of relevant progress in innovation and specific digital solutions. The FATF also looked at the persisting challenges and obstacles to their implementation and how to mitigate them. This project included the review and analysis of regulatory technology (RegTech) and supervisory technology (SupTech), both of which can improve the effectiveness of FATF Standards.

3. Innovative skills, methods, and processes, as well as innovative ways to use established technology-based processes, can help regulators, supervisors and regulated entities overcome many of the identified AML/CFT challenges. Technology can facilitate data collection, processing and analysis and help actors identify and manage money laundering and terrorist financing (ML/TF) risks more effectively and closer to real time. Faster payments and transactions, more accurate identification systems, monitoring, record keeping and information sharing between competent authorities and regulated entities also offer advantages.

4. The increased use of digital solutions for AML/CFT based on Artificial Intelligence (AI) and its different subsets (machine learning, natural language processing) can potentially help to better identify risks and respond to, communicate, and monitor suspicious activity. At public sector level, improved live (real-time) monitoring and information exchange with counterparts enable more informed oversight of regulated entities, helping to improve supervision. At private sector level, technology can improve risk assessments, onboarding practices, relationships with competent authorities, auditability, accountability and overall good governance whilst cost saving.

5. The report identifies challenges related to the development, adoption and application of these innovative solutions or practices. Many of these challenges are due to outstanding operational and regulatory constraints, such as legacy AML/CFT compliance systems and traditional regulatory frameworks and oversight mechanisms.

6. The complexities and costs involved in replacing or updating legacy systems make it challenging to exploit the potential of innovative approaches to AML/CFT for both industry and government. For industry, the cost-benefit analysis to adopt new technologies continues to be an obstacle to greater uptake of innovative solutions for AML/CFT, based in part on a real or perceived lack of regulatory incentives to pursue innovation. Difficulties with the explainability and interpretability of digital solutions are another key challenge for both industry and regulators that in part stems from the limited availability of relevant expertise and a lack of awareness of

innovative technologies' potential among AML/CFT professionals, both in industry and government. Increased communication and cooperation between the public and private sector, informed by the type of information and analysis provided by this report, together with an emphasis on responsible adoption of new technologies and effectiveness, in particular with regard to data protection regulations, will be key to overcoming these challenges and fully realizing the promise of responsible innovation to strengthen the effectiveness of AML/CFT measures.

7. When used responsibly and proportionally, innovative AML/CFT technologies can help identify risks and focus compliance efforts on existing and emerging challenges, but manual review and human input remains very important. For example, even in a technology enabling regulatory environment, human actors must be relied upon to identity and assess any residual risks presented by new technologies and put in place appropriate mitigation measures. Combining the efficiency and accuracy of digital solutions with the knowledge and analytical skills of human experts produces more robust systems that can effectively respond to AML/CFT requirements whilst being fully auditable and accountable.

8. The use of new technologies and innovation can help the public and private sectors improve the effectiveness of their risk-based implementation of the FATF Standards. The development, adoption and regulatory supervision of these technologies must reflect threats as well as opportunities. It must also ensure that the use of innovative tools is compatible with international standards of data protection, privacy, and cybersecurity.

1. Introduction

9. The FATF Standards are a dynamic tool that evolves in response to changing global money laundering and terrorist financing (ML/TF) threats, vulnerabilities and risks, and to challenges that occur in their implementation. Thirty years after their initial adoption, customer due diligence (CDD) and related procedures have greatly increased the transparency of transactions and made it harder for criminals, terrorist financiers, and weapons proliferator financiers to misuse financial products. At the same time, although customer identification/verification and monitoring is a key pillar of the AML/CFT framework, it continues to present challenges of implementation and effectiveness.

10. Non-risk targeted CDD efforts can be perceived to be costly and inefficient, as they consume and often do not translate into accurate risk assessment processes or smooth access to financial services. Recognising the accelerating pace of innovation, the profound impact of digital transformation on the financial system and the quest for greater effectiveness of FATF Standards, the FATF launched an initiative to examine the potential of new technologies to mitigate ML/TF threats.

11. For the purpose of this report, "new technologies for AML/CFT" [1] refers to:

    a innovative skills, methods, and processes that are used to achieve goals relating to the effective implementation of AMLCFT requirements or

    b innovative ways to use established technology-based processes to comply with AML/CFT obligations.

12. New technologies seek to improve the speed, quality, or efficiency and cost of some AML/CFT measures, as well as the costs of implementing the AML/CFT framework more broadly, compared to the use of traditional methods and processes. The technologies of greatest relevance are cross-cutting and enable new digital ways to collect, process, analyse data. These technologies also allow to communicate data and information via a variety of specific solutions. These capabilities can be applied in overlapping ways and target a broad range of AML/CFT objectives. Many of these new technologies' capabilities and implications are still largely unknown. That said, it is essential to understand their current capabilities and potential impact on AML/CFT.

13. For example, digital identity solutions can enable non-face-to-face customer identification/verification and updating of information. They can also improve authentication of customers for more secure account access, and strengthen identification and authentication when onboarding and transactions are conducted in-person, promoting financial inclusion and combating money laundering, fraud, terrorist financing and other illicit financing activities.

14. As another example, natural language processing can support more accurate, flexible and timely analysis of customer information and reduce inaccurate or false

[1] For the purposes of this report the terms *digital solutions*, *digital tools*, *innovative solutions* or *systems* are used interchangeably, and as appropriate, to mean new technologies for AML/CFT as defined in this paragraph.

information and enabling more efficient matching and search for additional data. Better and more up-to-date customer profiles mean more accurate risk assessments, better decision-making, and fewer instances of unintended financial exclusion.

15. Likewise, Artificial intelligence (AI) and machine learning (ML) technology-based solutions applied to big data can strengthen ongoing monitoring and reporting of suspicious transactions. These solutions can automatically monitor, process and analyse suspicious transactions and other illicit activity, distinguishing it from normal activity in real time, whilst reducing the need for initial, front-line human review. AI and machine learning tools or solutions can also generate more accurate and complete assessments of ongoing customer due diligence and customer risk, which can be updated to account for new and emerging threats in real time. However, AI/ML solutions vary greatly in both technology and use and may present significant risks, which are discussed later in this report.

16. Similarly, the adoption of innovative solutions, such as Application Programming Interface (APIs) and Distributed Ledger Technology (DLT), data standardisation, and machine readable regulations can help regulated entities[2] report more efficiently to supervisors and other competent authorities. The technologies also allow alerts, report follow-ups, and other communications from supervisors, law enforcement, or other authorities to regulated entities and their customers, as well as communications among regulated entities, and between them and their customers. The application of more advanced analytics by regulators can also strengthen examination and supervision, including by potentially providing more accurate and immediate feedback.

17. The embrace of new technologies for AML/CFT compliance and supervision has been impeded in some instances by concerns as to whether and how innovative technologies may be used under the FATF Recommendations, as well as under countries' AML/CFT regulatory frameworks.

1.1. FATF Commitment to Responsible Innovation and Digital Transformation

18. As a global standard setting body (SSB), the FATF is committed to keeping abreast of innovative technologies and business models in the financial sector and ensuring that the global AML/CFT standards remain relevant and effective in an environment of accelerating digital transformation. This is so FATF's requirements can enable "smart" financial sector regulation that helps drive responsible innovation to further both AML/CFT and financial inclusion objectives.

19. The FATF formally endorsed responsible innovation for AML/CFT in a public statement issued in Buenos Aires on 3 November 2017, which declared:

> "The FATF strongly supports responsible financial innovation that is in line with the AML/CFT requirements found in the FATF Standards, and will continue to explore the opportunities that new financial and regulatory technologies may present for improving the effective implementation of AML/CFT measures."

[2] For the purposes of this Report, 'regulated entities' refers to financial institutions, virtual asset service providers (VASPs) and designated non-financial businesses and professions (DNFBPs), as defined under the FATF Standards.

20. The 2017 public statement built on the FATF's prior efforts to support responsible innovation, while addressing potential illicit finance risks and the AML/CFT regulatory and supervisory challenges posed by emerging technologies. Those efforts include issuing numerous guidance and best practices papers, updating the Recommendations to address virtual assets (FATF, 2019[1]), and extensive engagement with the private sector through public-private workshops and the FATF Private Sector Consultative Forums (PSCF).[3]

21. Responsible innovation is supported through other international statements, namely the UN Security Council Resolution 2462(2019) (UN, 2019[2]) which called upon all States to enhance the traceability and transparency of financial transactions, including through fully exploiting the use of new and emerging financial and regulatory technologies to bolster financial inclusion, and to contribute to the effective implementation of AML/CFT measures.

22. Despite the acknowledged benefits, the effective use of innovative technologies for AML/CFT has been limited by a variety of factors, impacting different regulated entities and supervisors to different degrees.

23. Making innovation one of its top priorities, the FATF German Presidency launched a digital transformation initiative that includes three projects:

- The study underlying the present report, examining the opportunities and challenges of new technology to make implementing AML/CFT measures by the private sector and supervisors more efficient and effective;
- A study of opportunities and challenges for operational agencies, aimed at making systems to detect and investigate ML and TF and understanding ML/TF risks, more efficient, and
- A stocktake on data pooling, collaborative analytics and data protection, aimed at helping the private sector improve their use of AI and big data analytics for AML/CFT and increase the efficiency of regulatory compliance, while ensuring a high level of data protection.

24. The FATF President has brought this agenda to international fora, emphasising its importance for a better implementation of the FATF Standards and AML/CFT effectiveness. (FATF, 2020[3])

25. This report aims to:

- Increase awareness of and identify opportunities to leverage new technologies and emerging and existing technology-based solutions;
- Identify the conditions, policies and practices that can help support the further adoption of new technologies that contribute to the efficiency and effectiveness of AML/CFT efforts in line with jurisdictions' regulatory regimes, illustrated by case studies;
- Examine regulatory obstacles or other factors impeding the successful adoption of new technologies and where relevant, propose additional FATF projects to explore potential policy responses; and

3 Many of FATF's positions, engagement and relevant documents on FinTech and RegTech may be found at the FATF FinTech & RegTech Initiative website. Available at: www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/.

- Provide a common set of definitions, conceptual framework and suggested actions for government authorities and private sector stakeholders to advance the responsible development and use of new technologies for AML/CFT.

1.2. Scope and Methodology

26. This report focused on the ways in which new technologies may assist jurisdictions and regulated entities become more effective in the implementation of AML/CFT standards. In particular, digital solutions which enable a better understanding, assessment and mitigation of risks, customer due diligence and monitoring, and communication with supervisors may assist achieving effectiveness in the implementation of AML/CFT standards.

27. The report addresses the implementation of new technologies known as RegTech[4], such as AI, machine learning, big data, and advanced cognitive analytics/algorithms targeting customer identification and verification requirements, and broader AML/CFT compliance obligations. The project also considers SupTech[5] or technologies used by supervisory agencies, for example, risk assessment tools, data visualisation tools or others. (Coelho et al., 2019[4])

28. This report's research considers, where technologies have been deployed successfully, what were the preconditions which enabled their effective use, what were the benefits achieved, and what, if any, new requirements resulted from the successful use of innovative solutions?

29. The report also considers cases where promising technologies have not been successfully deployed and identifies challenges or obstacles to their effective use. It also explores whether coordinated global action is needed to enable greater use of innovative technology based solutions to support AML/CFT objectives. This includes analysing structural challenges, e.g. issues of data quality, changing legacy systems, cost constraints and the lack of regulatory incentives.

30. Where these technologies offer real benefit and help to respond to threats in an effective manner, FATF analyses use-cases from early-adopters of new technologies, to enable other regulated entities and authorities to implement them in the most effective way.

31. Examples of other technologies relevant to the better implementation of FATF Standards not proposed for analysis in this report include:

- Data management and sharing tools
- Analytic tools including the use of machine learning and big data analytics by FIUs

---

4 RegTech is a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities, as referred to in Feedback Statement FS16/4, Financial Conduct Authority, *Call for Input on Supporting the Development and Adopters of RegTech* (2016). Available at: www.fca.org.uk/publication/feedback/fs-16-04.pdf

5 Supervisory technology (suptech) is the use of innovative technology by supervisory agencies to support supervision. See, (Broeders D. and Prenio J., 2018[36])

32. This report relies on general desk-based research and responses to an online digital transformation Questionnaire[6] which the FATF Secretariat disseminated to government authorities and public and private sector experts. The Secretariat also consulted with key stakeholders to obtain additional information and expert views, including at a High-Level Roundtable on the Opportunities and Challenges of New Technologies for AML/CFT held virtually by the FATF on 10 of March, 2021.

33. The FATF Digital Transformation questionnaire sought stakeholders' views on the main users (adopters) of new technologies, the purposes and added value of given technology-based solutions under the jurisdiction's AML/CFT and other regulatory frameworks. It also focused their impact on users' relationships with the supervisors and obstacles to implementation, and the relationship of new technologies to the FATF Standards and other regulatory frameworks. It also encouraged respondents to submit case-studies illustrating best practices and/or specific challenges. 54% of respondents identified as private sector representatives, mainly large banks and technology developers. At public sector level, the majority of responses were submitted by supervisors.

6 The Questionnaire sought information on the opportunities and challenges of new technologies for this project. It collected 188 responses, including case-studies and examples of digital solutions'.

2. New Technologies for AML/CFT: towards a more effective implementation of FATF Standards

34. One of the main challenges hindering the effective implementation of AML/CFT measures is poor understanding of ML/TF threats and risks. Decision-making, based on inadequate risk assessments is sometimes inaccurate and irrelevant, relying heavily on human input and defensive box-ticking approaches to risk, rather than applying a genuinely risk-based approach.

35. The inability to adequately identify, assess and mitigate money laundering and terrorist financing risk, including the fundamental elements of risk identification (customer identification/verification and monitoring of transactions) poses an obstacle to effectiveness in AML/CFT. This is where new technologies can provide the most added value.

36. The majority of current risk assessment and risk management efforts are based on a combination of automated but static analyses of a pre-determined set of risk factors, together with human judgement. Legacy systems[7] are updated with new algorithms and manually inputted information, generating matrixes for risk interpretation and action, but these very rarely offer a real time overview of customer transactional or institutional risks.

37. Moreover, traditional risk assessment tools, based on spreadsheets (such as Excel) or static reporting platforms, do not allow data to be analysed at a large scale, limiting the potential for correlations and analysis to generate a more fine-grained picture of the risks. In addition, the quality of the data obtained by legacy systems varies and may not offer the accuracy and detail required to comply with AML/CFT standards.

38. In the private sector, poor risk assessment can lead to a defensive box-ticking application of the AML/CFT framework, which is inefficient and burdensome, and more importantly does not reflect the real ML/TF threats to the institutions. Poor risk assessment undermines a genuine risk-based approach to decision-making and protecting the integrity of the financial system. This potentially contributes to two distinct problems - lack of sufficient attention to mitigating new or emerging risks (allowing ML and TF to take place), and over-application of risk mitigation measures in low-risk situations where simplified measures may be appropriate (causing unnecessary costs and friction to customers, including financial exclusion).

39. The use of new technologies in the identification, assessment and management of ML and TF risks allows risk analysis to be more dynamic, provide network analysis, and operate at customer, institutional, jurisdictional and cross-border levels (See Box 1). However, optimal use of these tools requires a regulatory and policy environment that frames adequate data pooling and sharing, or collaborative analytics, as well as appropriate access by supervisors and law enforcement.

7 For the purposes of this paper "legacy systems" refers to the systems and practices that rely on *low-tech (manual submissions and databases)* processes for data collection and analysis.

Box 1 Dynamic risk assessment tool for FIs

A multinational FI is building a Dynamic Risk Assessment tool to:

- Use data with greater depth and richness updated dynamically to reflect the latest investigative insights.
- Identify financial crime risk at a faster pace and with less unproductive alerts.
- Create more accurate and sophisticated assessment of customer risk.

This tool uses cloud capabilities to centralise and process data at scale. It also includes new techniques, including-machine learning, to identify financial crime risk through:

- Incorporating existing knowledge on financial crime typologies and suspicious activity.
- Looking at an entity's transactional and social links to other entities with suspicious or confirmed adverse characteristics.
- Quantifying (or capturing) an entity's abnormal behaviour with respect to peer groups of similar characteristics.
- Quantifying (or capturing) an entity's abnormal behaviour with respect to its own historical behaviour.

40. Difficulties in identifying, understanding and managing risks negatively impact both the public and private sector entities surveyed. An analysis of 4th Round FATF Mutual Evaluation Reports (MERs) showed that many supervisors are still unable to carry out proper risk assessments of the supervised entities by sector or at institutional level. The MERs analysed suggest that many supervisors lack the ability to collect and process data because of resources and tool shortages. Some supervisors' risk assessments lack adequate updating and the needed critical basis needed for the adoption of the risk-based approach, and for providing adequate feedback to supervised entities.

41. While the numbers of digital identity and AML/CFT transaction monitoring and reporting solutions are increasing, and RegTech firms have proliferated (see Annex D), respondents confirmed there is still a significant gap in supervisors' and regulators' capacity and adoption of these technologies.

Box 2. Dynamic risk assessment tool for Supervisors: a digital solution for risk assessment

A commercial-off-the-shelf (COTS) SupTech tool for FI or DNFBP supervisors automates the AML/CFT risk assessment process, usually performed on an annual basis, to inform the supervisory engagement for a given cycle.

The COTS tool supports a Risk-Based Approach with three modules:

- a data collection module for data quality assurance and survey management,
- a scoring module with a risk model that imports survey data, scores Inherent Risk, and combines it with an assessment on quality of Controls to generate Residual Risk ratings on the institutional level, and
- a data analysis module to provide supervisor-relevant analyses over sectors, sub-sectors, individual entities, and individual risk factors.

The COTS tool uses an organically developed risk model incorporating the machine learning concept of *dimensionality reduction* in the risk scoring algorithm. The scoring algorithm right-sizes the risk model for each entity by reducing model variables (risk factors) to those reported with significant activity, eliminating the 'water-down effect'. As a benefit, this identifies risky narrow business models and small-but-risky entities.

This solution identifies risk with more relevance and precision, and produces residual risk results faster and at a lower operating cost, than non-automated alternatives.

2.1. Implementing the risk-based approach

42. "*The risk-based approach should be the* cornerstone *of an effective AML/CFT system, and is essential to properly managing risks*". (FATF, 2014[5]) Nevertheless, despite FATF Guidance (FATF, n.d.[6]) to this end, the FATF Strategic Review of the 4th Round of Mutual evaluations concluded that many jurisdictions continue to apply largely rule-based systems. Similarly, the private sector continues to struggle to adopt the risk-based approach, preferring a costly and defensive approach to AML/CFT.

43. A robust knowledge and awareness of risks, which allows for the capacity to mitigate and address risks proportionately is crucial to the effective implementation of FATF Standards.

44. The traditional, rule-based approach has led to defensive compliance, rather than the application of different mitigating measures to different levels of risk. The authorities' response to over reporting in relation to under reporting has further contributed to defensive actions.

45. Defensive AML/CFT frameworks are the result of regulatory or operational uncertainty and/or lack of trust in the strategies and mechanisms applied. Public and private sectors alike may lack trust in their own risk assessments because of their incomplete understanding of reality, lack of information and data, and lack of resources and tools to carry out solid, up-to-date and comprehensive risk assessments.

46. A greater capacity to collect and process data, as well as share it among stakeholders, could offer significant advantages in this area, as it would promote a more dynamic risk-based approach.

47. The application of machine learning and other AI based tools which allow for real-time, quick and more accurate data analysis may offer the solution to the issues identified above. Such tools can partially or fully automate the process of risk analysis, allowing it to take account of a greater volume of data, and to identify emerging risks which do not correspond to already-understood profiles. Such tools can also offer an alternative means of identifying risks - in effect acting as a semi-independent check on the conclusions of traditional risk analysis.

48. Even when, the conclusions reached using such tools are the same as those resulting from traditional risk analysis, this confirmation can reassure actors of the completeness and accuracy or their assessments. In this way, machine learning can increase their degree of confidence when applying risk based measures – and allow them to more comfortably justify the use of such measures to their supervisors. Automated risk assessment tools may also be more readily auditable by supervisors and offer increased objectivity.

49. Implementing new technologies to resolve these weaknesses requires technical work. However, the primary obstacles are some of the existing supervisory practices and the difficulties some supervisors face to innovate, as reported by respondents. Nevertheless, the case study in Box 3 demonstrates that the desired culture shift is emerging and some supervisors are already engaging with the sector to encourage the adoption of new technologies.

Box 3. FinCEN and the Federal Banking Agencies

The Federal Banking Agencies (FBAs) and FinCEN issued a "Joint Innovation Statement" in December 2018, encouraging industry to consider, evaluate, and where appropriate, responsibly implement innovative approaches to AML/CFT obligations, while still complying with Bank Secrecy Act (BSA)/AML compliance obligations. The Statement focuses on AML (transaction monitoring) compliance solutions, but also includes innovation solutions to comply with BSA/AML requirements more broadly, including innovative digital identity solutions. It recognizes that private sector responsible innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity by enhancing the effectiveness and efficiency of banks' BSA/AML compliance program.

The Statement seeks to provide assurance that AML pilot programs that are designed to test and validate the effectiveness of responsible innovative approaches will not, in and of themselves, necessarily result in:

1) supervisory criticism, if the pilots ultimately prove unsuccessful;
2) supervisory action if a pilot exposes gaps in an existing AML compliance program; or
3) additional regulatory expectations if innovative approaches are implemented.

The Statement also made clear that FinCEN will use its exceptive relief authority to support responsible AML/CFT innovation pilots that may not otherwise be possible because of a specific regulatory prohibition or impediment.

The Statement also encourages the private sector to engage with the Agencies on their innovative pilot programs for innovative BSA/AML approaches, highlighting early engagement can promote a better understanding of these approaches by the Agencies, and allow for the clarification of supervisory expectations as appropriate and as needed.

2.2. Financial Inclusion

50. Promoting financial inclusion is an important part of the effective implementation of the FATF Standards and can reduce ML/TF risks overal. However, mitigating financial exclusion continues to pose a challenge.

51. Around the world, one billion people struggle to provide adequate identification documents for opening bank accounts or maintaining access to financial services. (Vyjayanti T Desai et al., 2018[7]) Even when identification is possible, CDD procedures along with strict and box-ticking implementation of risk management practices lead to the financial exclusion of often the most fragile segments of societies.

52. The majority of respondents agreed that protecting the rights of individuals to access financial services and ensuring financial inclusion are key elements of an adequate implementation of AML/CFT and that, in order to be effective, the mitigation and avoidance of such unintended consequences should be a priority.

53. FATF has reiterated its commitment to the proportionate risk-based adoption of its Standards with a view to protecting the most vulnerable and supporting the reach of AML/CFT safeguards. Its publication of FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence sought to raise awareness of the issue as well as "*encourage countries to make use of the FATF Recommendations' flexibility to provide sound financial services to the financially excluded.* (Vyjayanti T Desai et al., 2018[7])

54. The more recent FATF Guidance on Digital Identity (FATF, 2020[8]) also includes detailed information on the use of a risk-based approach to digital identity solutions to support financial inclusion.

55. The G20 High Level Principles for Digital Financial Inclusion, (G20, 2016[9]) emphasised financial inclusion confirming the need for a proportionate and risk-based approach to identification requirements aided by digital tools and financial literacy.

56. The FATF's work is reinforced by the work of the United Nations that promotes and supports the responsible use of biometric data for counter terrorism purposes, with the aim of preventing unintended consequences and respecting international law. (UN, 2018[10])

57. A key element to securing financial inclusion is the implementation by financial institutions of effective, risk-based approaches to AML/CFT, including CDD requirements. (EBA, 2021[11]) CDD underpins the assessment of the risk associated with individual customers in place of a rigid, box-ticking approach and indiscriminate policies for broad categories of customers. Innovative technology-based solutions – both digital ID and AML compliance transaction monitoring tools - can facilitate more accurate and up-to-date risk assessments at an optimised cost and provide greater confidence in the conclusions of that risk assessment, enabling greater use of simplified due diligence where appropriate. This could be a significant enabler of financial inclusion, which has to date been held-back by unwillingness to make full use of the flexibility offered under the risk-based approach, as well as by profit-based business decisions of financial institutions.

58. Innovative technology-based solutions may contribute to financial inclusion, as long as they are implemented through a responsible (Chase, 2020[12]) and risk-based approach. They can minimise weaknesses in inconsistencies related to human control measures, improve customer experience, improve customer experience, generate cost savings, and facilitate transaction monitoring as summarised in Box 4.[8] Traditional ID requirements (Kazzaz, 2020[13]) may be the most obvious instrument to identify customers but should not be the only tool used for this purpose.[9] For example, natural language processing tools, the use of biometrics and other similar instruments[10] may be more beneficial to the CDD process than forcing in-person production of physical ID documents, notwithstanding the role and review of human analysts and experts which remains key to prevent bias and other unintended consequences of over-technology reliance.

8 For more on the benefits of digital ID please see (FATF, 2020[8]).

9 Please refer to previous FATF publications on Digital ID www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html and COVID-19 www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html for relevant recommendations on the use of digital financial services.

10 Broadly known as "digital ID" referring to the body of information about an individual, organization or electronic device that exists online.

Box .4. Benefits of digital ID for financial inclusion for regulated entities and individuals

For regulated entities:

1. Lowering costs: Digital ID can support cheaper and more sophisticated processes for customer onboarding. In particular, combined with increased possibilities to access financial services via mobile devices and smartphones, technology can radically change the way consumers are able to access financial services. Cheaper and more automated CDD processes that allow wider data sets and sources can allow customers with no traditional credit record to access financial services or automated brokerage services – and make such services more affordable.
2. Portability and interoperability. Systems can be used across multiple institutions or transactions reducing the burden of verification to one instance of onboarding only (offering particular advantages if the initial verification is government led).
3. Reducing human error. While human input may still be required and desirable, the automation of data collection and matching allows for the consideration of many more data points in a shorter time frame than would be possible to carry out manually.

For individuals:

4. Better customer experience: Digital ID greatly reduces the burden of in person ID and, for example, the need to carry and submit multiple documents in physical form.
5. Multiple use: Systems that allow for multiple use of verified ID simplify daily operations and offer greater efficiency to interactions with service providers and authorities.

59. Technology can also enable financial inclusion through enhanced digital tools for transaction monitoring. As set out in the guidance on financial inclusion, enhanced ongoing monitoring can be used to manage the ML/TF risks associated with the trustworthiness of customer identification and verification data, so that ML/TF risk management is not so heavily reliant on CDD at the time of customer onboarding. For example, in cases where customers are able to provide only less reliable forms of evidence of identity – and therefore identification and verifications elements are not sufficiently robust – technological solutions, such as behavioural analytics, may support a strengthened and enhanced transaction and business relationship monitoring, thereby enabling customer take-on. These technologies can also give a robust ongoing monitoring process and provide a better understanding of risk.

60. The development of technology-based solutions in this context could facilitate "white labelled" transactions (e.g. salary, payments for utilities and living expenses, government support payouts etc.) and also be used to enhance limited accounts if and when the customers' risk assessment allows. This would enable more

customers to have access to basic banking services, while mitigating the risks faced by the financial institutions. Nevertheless, it is important to ensure that CDD, at account opening, provides sufficient information to inform effective customer monitoring, which has implications in terms of the amount of information to be collected. Monitoring will not be an effective control if an institution has too little information about its customers and their expected use of the relevant financial products.

61. In addition, improvements in transaction monitoring may ease financial exclusion if they give greater confidence to banks that other kinds of financial institutions, such as MVTS providers, employ robust compliance programs. Better risk assessments, CDD procedures and adequate monitoring tools could become an important part of more inclusive and safe financial systems that do not discriminate on the basis of means, social or regional context.

62. Digital solutions for financial inclusion purposes, e.g. biometrics, are not without their own challenges. There are also risks that such processes can exacerbate financial exclusion in sectors of the population that do not have access to electronic devices, trust or awareness of the possibilities these create, especially where financial services providers develop digital only business models. Some of the current strategies implemented to promote financial inclusion may also lead to a delay in the exclusion process. Limited accounts[11] may restrict the type of activity or function expected from a bank account and lead to unsatisfactory customer experiences and a subsequent exit from the formal banking system. Remote onboarding, account tiers, and deferred identity proofs have also been identified as sometimes leading to additional difficulties in fully accessing financial services. (Kazzaz, 2020[13]) In this context, innovation can also help to mitigate the unintended consequences of reliance on new technologies by offering alternatives to financial institutions' monitoring of banking relationships. Behavioural risk profiles, network analysis and the use psychometric data could, for example, inform underwriting and access to credit becoming a powerful complement to the benefits generated by digital ID systems.

63. It is important that the use of such approaches also create a route towards full-service and un-limited access to financial services, where possible. The solutions noted above have some potential to enable this transition (e.g. technology-enhanced ongoing monitoring over an extended period, and behavioural analytics, can give a more robust basis for customer risk profiling and improve the effectiveness of enhanced due diligence related to the lack of trustworthiness of customer identification and verification, potentially allowing to extend the functions of the aforementioned accounts).

64. Ultimately, any adoption of new technologies for AML/CFT purposes must follow a problem-solving approach which is equally aware of not creating additional burden or unintended consequences.

[11] Limited or basic accounts are minimum services accounts designed to provide access to financial services. These account often have limits on the value of transactions, the ability to access credit and online banking tools or payment systems.

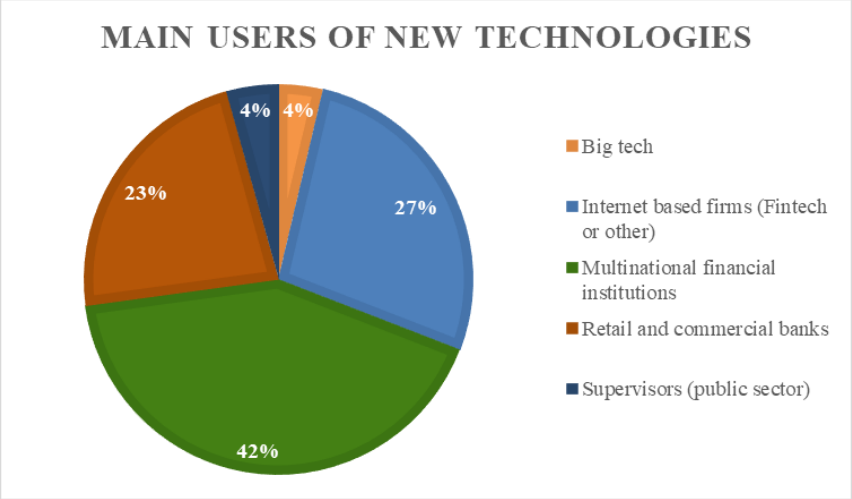
3. The Opportunities of New Technologies for AML/CFT

65. The FATF's Digital Transformation questionnaire sought information about how new technologies are being developed and deployed for AML CFT, including:

- *Who* is using new technologies?
- What AML/CFT functions are they are being used for?; and
- Which underlying technologies are being used to perform those functions?

66. On the question of *who* is using new technologies, FIs, technology developers and FinTech regulated entities of multinational scale have led the demand for new technologies, as illustrated by Figure 1.

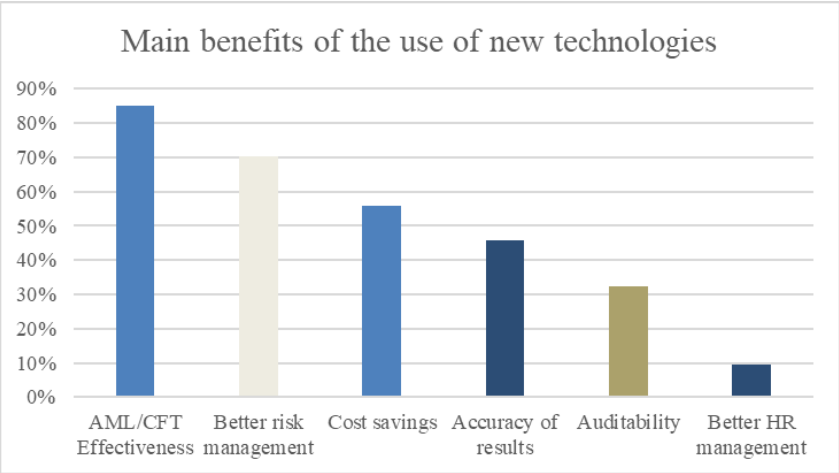
Figure 1. Main Users of New Technologies



67. Respondents believe that the adoption and demand for new technologies has been unequal and that significant gaps continue to exist between large financial institutions and smaller actors, but also at a regional and national level, with smaller economies falling behind of digital innovation.

68. On the question of *What* AML/CFT functions are they are being used for, new technologies promise to increase the effectiveness of AML/CFT efforts by proving stakeholders with faster and more cost efficient tools. 85% of respondents agree that AML/CFT effectiveness in general is the most significant benefit of the use of new technologies, while better risk management follows in relevance, as illustrated in Figure 2. Respondents declared speed, flexibility, capability and better governance as the outcomes of new technologies contributing to greater AML/CFT effectiveness.

Figure 2. Main Benefits of the Use of New Technologies



69. Respondents stressed a greater use of new technologies by supervisors as likely to contribute to AML/CFT effectiveness through the enhancement of supervisory capabilities. Advantages of new technologies for supervisors mentioned by experts include the ability to:

- Supervise a larger number of entities[12];
- Better identify and understand the risks associated to the different sectors individual entities;
- Live monitor compliance with AML/CFT standards and act in cases of non-compliance;
- Communicate more efficiently with the supervised entities and carry out additional information requests;
- Store, process and report on larger sets of supervisory data;
- Exchange information with other competent authorities.

70. Advantages for the private sector include the ability to:

- Better identification, understanding and management of ML/TF risks;
- The ability to process and analyse larger sets of data in a quicker, speedier and more accurate manner;
- More efficient onboarding practices (digital);
- Achieve greater auditability, accountability and overall good governance;
- Reduce costs and maximise human resources to more complex areas of AML/CFT;
- Improve the quality of suspicious activity report submissions.

12 The increased number of supervised entities as a consequence of digitalisation is identified as one of the demand drivers for the use of Suptech. Others include the need for more accurate data, increased complexity of regulations, improved risk management capabilities, and more insightful policy and forward looking supervision. (FSB, 2020[14])

71. At a more granular level, respondents highlighted the ability of new technologies to provide results and data processing results that not only go beyond human capability to process large volumes of information in record time, but also are more reliable and easier to communicate to others, as a result of data standardisation and matching software.[13]

72. RegTech was identified by 52% of respondents as the AML/CFT area where the majority of benefits from new technologies may be secured.[14] In particular, respondents confirmed the processing and analysis of large data sets required for risk assessments and analysis, CDD, as well as transaction monitoring, as the areas securing the greatest benefits from new technologies.

73. Respondents stressed the ability of new technologies to enhance AML/CFT capabilities and release human resources for more critical work such as the analysis of complex ML/TF cases. Data management, including the ability to collect, analyse and use information in a useful but cost efficient way was a cross cutting element of responses.

74. New technologies were furthermore described as allowing the information held in internal systems to be more accurate, although a few respondents stressed the importance of constant review and the fact that machine learning implies *learning* from human actions and decisions, and from existing institutional practices.

75. The element of timeliness and the ability to continuously keep data analysed and updated without the need for human intervention was also highlighted as a key advantage; in particular, as regards legacy systems and the ability to update customer records. This is particularly relevant for natural language processing tools, which allow for the matching of customer records despite differences in spelling or error in the original data insertion.

76. On the third question - which underlying technologies are being used to perform those functions, the questionnaire asked which technologies have the most potential for contributing to AML/CFT effectiveness. Responses identified AI (to include machine learning and natural language processing tools), Application Programming Interfaces (APIs), and tools used for the purpose of CDD as having the most potential.

77. Distributed Ledger Technology (or Blockchain technology) was mentioned in the early stages of this work as potentially relevant but found to have a lower level of adoption by respondents. Nevertheless, a few examples of specific DLT based projects – mostly still in the developing phases - are illustrated below.

3.1. Artificial Intelligence (AI)

78. AI is the science of mimicking human thinking abilities to perform tasks that typically require human intelligence, such as recognizing patterns, making predictions recommendations, or decisions. AI uses advanced computational techniques to obtain insights from different types, sources, and quality (structured and unstructured) of data intelligence to "autonomously" solve problems and

13 For more on the role of information sharing see (FATF, 2020[37])

14 The EBA 2019 survey on Regtech showed that a significant share of banks included in the sample (42%) implemented at least one RegTech solution. Available at: https://www.eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub/regtech-industry-survey

execute tasks. There are several types of AI, which operate with (and achieve) different levels of autonomy, but in general, AI systems combine intentionality, intelligence, and adaptability.

79. *Machine Learning* is a type (subset) of AI that "trains" computer systems to learn from data, identify patterns and make decisions with minimal human intervention. Machine learning involves designing a sequence of actions to solve a problem automatically through experience and evolving pattern recognition algorithms with limited or no human intervention — i.e., it is a method of data analysis that automates analytical model building. Respondents cite machine learning and natural language processing as the AI-powered capabilities offering great benefit to AML/CFT for regulated entities and supervisors (see Box. 5). Machine learning reportedly offers the greatest advantage through its ability to learn from existing systems, reducing the need for manual input into monitoring, reducing false positives and identifying complex cases, as well as facilitating risk management.

Box 5. Supervisory uses of machine learning

Brazil

Supervision processes

In 2019, the Central Bank of Brazil (BCB) Conduct Supervision developed a priority matrix from a set of objective indicators in order to identify which supervised entities should be prioritized in the Annual Supervision Planning (ASP). This priority matrix was used for the first time in 2020, as input for the 2021 supervision planning (as a prototype).

The BCB is using machine learning to improve the priority matrix to support its ASP within the framework of a risk-based approach. The unsupervised learning technique is being used to calculate the supervised entities' risk score.

80. Machine learning applications are useful for detecting anomalies and outliers identifying and eliminating duplicate information to improve data quality and analysis. For example, Deep Learning (DL) is an advanced type of machine learning in which artificial neural networks (algorithms inspired by the human brain) with numerous (deep) layers learn from large amounts of data in highly autonomous ways. DL algorithms perform a task repeatedly, each time tweaking it a little to improve the outcome, enabling machines to solve complex problems without human intervention.

3.2. Natural Language Processing and soft computing techniques

81. Natural language processing (NLP) [15] is a branch of AI that enables computers to understand, interpret and manipulate human language. Fuzzy logic is a logical technique that takes imprecise or approximate data and processes it using multiple values, in a way that produces a useable (but imprecise) output. Such logics are non-binary, using a range of values instead of only 0 or 1. Fuzzy Logic systems can produce useful output in response to incomplete, ambiguous, distorted, or inaccurate (fuzzy) input, simulating human decision making more closely than classical logic, and extracting more useful information from data that is too imprecise to enable definite results to be derived using classical logic. Fuzzy logic can be implemented in hardware, software, or a combination of both.

Box 6. Fuzzy logic applications

Italy

Italy's Financial Intelligence Unit (UIF) in cooperation with the Directorate General for Financial Supervision and Regulation of Bank of Italy built an application of fuzzy logic for the construction of AML indicators for non-banking financial intermediaries. The proposed fuzzy system – currently at an experimental stage - allows to elaborate quantitative data (i.e. cross-border payments from/to higher risk countries) in order to support the periodical AML/CFT risk assessment of such intermediaries.

The source of data used for computing the indicators is the aggregate anti-money-laundering reports (S.AR.A. from the Italian acronym) database and Supervisory reports. For the construction of the indicators, non-banking financial intermediaries are split in different classes according to their typology (e.g. investment regulated entities, asset management companies, payment and electronic money institutions, credit providers) and main activity (e.g., open funds, closed funds, money transfer, electronic money and other payment services, etc.).

82. Natural language processing and fuzzy matching tools also allow for a more efficient reduction of false positives and negatives (e.g. in sanction screening processes) but chiefly overcomes problems of data quality, as the programmes become better at linking elements of information, for example, connecting search engine results with PEP lists, identifying fraud attempts, monitoring sanctions lists, etc. as illustrated in Box.7.

15 "Natural language processing (NLP) is a branch of artificial intelligence that helps computers understand, interpret and manipulate human language. NLP helps computers communicate with humans in their own language, making it possible for computers to read text, hear speech, interpret it, measure sentiment and determine which parts are important." (SAS, n.d.[15])

Box 7. Natural Language Processing in practice

Brazil

The Central Bank of Brazil (BCB) approved a Natural Language Processing (NLP) SupTech Project in April 2020, with the aim of incorporating AI applications for document processing based on NLP techniques for supervision purposes.

With this project, the BCB intends to further mitigate the risk of non-compliance with its supervisory attributions, established in its legal and regulatory framework, and to increase supervision productivity.

Tools under development include the analysis of:

- Social media: capturing texts as an ancillary source of information for supervision activities;
- Internal reports and documents: classification and summary of the Supervised Entities´ (SEs) responses in the scope of the AML/CFT remote inspections stored in the web-based system (SisAPS – more details available on Annex C) in order to increase the processing capacity of the qualitative information presented, providing an improvement in the supervision's requests;
- External reports and documents (explanatory notes, audit reports, relevant facts and minutes of boards): research, summarization and classification of relevant information to the Supervision, such as qualitative information in explanatory notes from audit reports;
- Global internet research (web scrapping): scanning of public data for analysis, construction of indicators and/or formation of databases in order to extract information related to SEs involved with ML/TF. In a second phase, machine learning will be used to read the news and extract from them evidence of legal entities involved in trade-based money laundering (TBML);
- Automation of reports - Inspections and follow-ups: automated generation of descriptive texts of the working papers and reports for use in inspections.

83. Broadly, the application of AI to AML/CFT processes may enhance the capabilities of actors to respond to risks and implement requirements more effectively. These tools are not a replacement but rather a complement to the systems aimed at improving results and simplifying compliance.

84. Transaction monitoring using AI and machine learning tools may allow regulated entities to carry out traditional functions with greater speed, accuracy and efficiency (provided the machine is adequately and accurately trained) (See Box.8). These models are useful for filtering the cases that require additional investigation. The use of new technologies for monitoring purposes should, for the most part,

continue to be integrated with the broader monitoring systems which include an element of human analysis for specific alerts or areas of higher risk. These systems must also improve their degree of explainability and auditability in order to fully comply with the majority of supervisory requirements.

Box 8. Where can machine learning add value?[1]

- *Identification and Verification of customers:* In the context of remote onboarding and authentication AI, including biometrics, machine learning and liveness detection techniques can be used to perform: micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis.
- *Monitoring of the business relationship and behavioural and transactional analysis:*
    - *Unsupervised machine learning algorithms*: to group customers into cohesive groupings based on their behaviour, which will then create controls that can be set more adequately based on a risk-based approach (ex: transaction threshold settings), allowing a tailored and efficient monitoring of the business relationship.
    - *Supervised machine learning algorithms:* Allow for a quicker and real time analysis of data according to the relevant AML/CFT requirements in place.
    - *Alert Scoring:* Alert scoring helps to focus on a patterns of activity and issue notifications or need for enhanced due diligence.
- *Identification and implementation of regulatory updates:* Machine Learning techniques with Natural language processing (NLP), cognitive computing capability, and robotic process automation (RPA) can scan and interpret big volumes of unstructured regulatory data sources on an ongoing basis to automatically identify, analyse and then shortlist applicable requirements for the institution; or implement (to a certain extent) the new or revised regulatory requirements (via codification and generation of implementation workflows) so regulated entities can comply with the relevant regulatory products.
- *Automated data reporting (ADR):* the use of standardised reporting templates using automated digital applications (data pooling tools) making the regulated entities underlying granular data available in bulks to supervisors.

1. Non-exhaustive list

3.3. Distributed Ledger Technology

85. DLT may improve traceability of transactions on a cross border basis, and even global scale, potentially making identity verification easier. A responsible and regulated use of DLT for data and process management purposes may also speed up the CDD process, as consumers can authenticate themselves and can even be automatically approved or denied through smart contracts that verify the data (See Box 9).

86. In addition, under appropriate safeguards and regulatory environment, transactions can potentially be managed via a single ledger shared among several institutions across jurisdictions, or via interoperable ledgers. This would significantly increase the monitoring possibilities compared to the existing frameworks. It also means that, as DLT becomes more widely understood and accessible, contractual arrangements, for example, could be built into securities as they are issued via smart contracts, which means that every time a transaction in securities is initiated, other shareholders would be automatically notified and could become – dependent on the contract design – counterparties in the transaction..

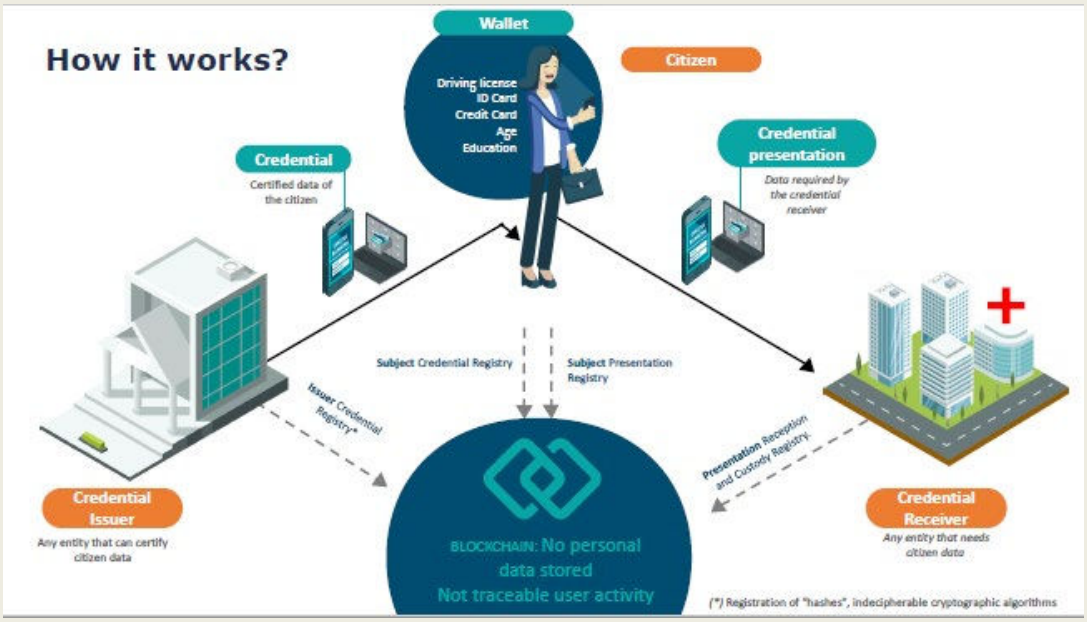
87. DLT technologies may also offer benefits for managing CDD requirements contributing to user concerns regarding this process, greater cost effectiveness for the private sector, and a more accurate and quality-based data pool. For example, in China, DLT is being used by financial institutions to share watch lists or red flags on the basis the scope of confidentiality permitted by this system.

88. Despite its merits, DLT seem to continue to pose challenges and raise significant concern from an AML/CFT perspective, as seen in the regulation and /supervision of virtual assets.[16] Unlike transactions through conventional intermediaries such as banks, transactions in virtual assets (VA) based on DLT are decentralized in nature and enable un-intermediated peer to peer transactions to take place without any scrutiny. They also pose jurisdictional challenges, if there is no single entity or clear location responsible for the activity. This could pose potential challenges to traditional FATF standards that have focused on regulating/supervising intermediaries. The use of this technology should therefore be monitored and further considered by FATF members in detail. Authorities may also want to consider the carbon footprint of using DLT compared to traditional tools.

[16] See (FATF, 2021[38]) section V

Box 9. CDD and DLT

A collaborative initiative with nine large private companies from different industries and support from local supervisors, this entity promotes a model for managing digital identities from a user controlled perspective (self-sovereign identity). It follows European and Spanish standards to grant interoperability with future alternatives. Because it uses DLT, this system allows for the user to control operations from a "wallet" which simplifies exchanges and ID and CDD procedures with partner entities. This project is in pilot phase and expects to enter production in 2021.



3.4. Digital Solutions for Customer Due Diligence

89. Customer identification/verification and monitoring is a key pillar of the AML/CFT framework but, in some instances, continues to present challenges of implementation and effectiveness. When implemented on a non-risk basis these efforts are believed to be costly and mostly inefficient as they consume resources and time which is often not translated into accurate risk assessment processes or into successful business relationships.

90. According to the private sector parties surveyed, CDD measures and monitoring make for an extremely burdensome process whilst still generating high-levels of uncertainty in data quality, difficulties in updating and matching information as required. CDD procedures are also among the main sources of dissatisfaction for customers. The process of collecting and verifying information is often difficult and strenuous, filled with endless requests for documents and additional in person periodic evidence submissions. In addition, experts mention the risk analysis generated by CDD is too rule-based rather than behavioural or contextual leading to the financial exclusion of unprivileged individuals or groups, who struggle to comply with the requirements.

91. The application of new technologies to CDD and monitoring may contribute to solving these challenges through more streamlined *onboarding* processes adapted to the risk, context and individual without compromising the integrity of the entity providing the service or the financial system. These have the potential to improve the customer experience, as well as contribute to more effective AML/CFT safeguards. For example, evidence suggests, that mixed approaches, where official ID's are provided in tandem with biometric identification may offer more robust identification and verification processes.

92. Digital ID provides one of the best case studies for this area, as it has been widely adopted and supported in many jurisdictions (and FATF has issued guidance on its use). Evidence suggests that the COVID-19 crisis has further promoted demand for remote financial services delivery. In fact, eID and verification is among the "most mature and instantly useful elements of technology in AML". (Richard Grint et al, 2017[14]) It is also among the most recognizable and often mentioned by respondents to the questionnaire as a good practice in AML/CFT (See Box 10).

93. Digital ID may improve, for example, customer access to financial services through mobile devices and smart phones whilst ensuring the security and accuracy of customer information through biometric information as a supplement to personal identity information. Some financial institutions may, based on basic ID information, increase the diversity of data sources by collecting additional data from customers, with their permission, which ultimately strengthens the knowledge and ability to manage the business relationship.

Box 10. Digital Identification solutions

eIDAS Regulation

The eIDAS Regulation is the first global cross-border framework for trusted electronic identification and trust services. The regulation allows for eIDs issued in one EU Member State to be used to access online public services in another Member State. Trust services are electronic services that aim to make electronic business transactions more secure, convenient and efficient. Trust services under eIDAS include electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication. eIDAS establishes harmonised rules and a process to develop a European internal market for trust services recognised across borders with the same legal status as their traditional equivalent paper-based processes.

India - eKYC

India has implemented a system for electronic verification of credentials of a customer – eKYC (electronic Know your Customer). This system is implemented through Aadhaar, a 12-digit identification number issued by Unique Identification Authority of India (UIDAI). While enrolling with Aadhaar, details like name, address, gender, date of birth, mobile number and email address are captured and incorporated in the

database of UIDAI.

FIs can use the eKYC Application Programming Interface (API) to get access to the Aadhaar details for verification and UIDAI ensures that FIs comply with the established standards of safety, security, and privacy while handling the data.

The authentication of the customer is done through a *One Time Password* sent to the recorded mobile number, or through biometrics. These provisions for eKYC have been incorporated in the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 (PMLR) in 2019. "e-KYC authentication facility" has been defined under Rule 2(1)(ca).

CKYC

India has implemented a Central KYC Register (CKYC), a centralized repository of KYC records of customers in the financial sector with uniform KYC norms to allow inter-usability.

CKYC is managed by CERSAI (Central Registry of Securitization Asset Reconstruction and Security Interest of India) and avoids customers having to perform KYC formalities with multiple FIs ahead of establishing business relationships.

CKYC has been incorporated in PMLR in 2019 and is defined under Rule 2(1)(ac).

Singapore – MyInfo

Singapore launched the first National Digital Identity service in 2017, known as MyInfo, which contains government-verified data retrieved from various Government agencies. By consenting to the use of MyInfo, it allows residents and corporates to share verified data with businesses, thereby minimising the need for businesses to obtain additional physical or electronic documents for processing.

Using MyInfo to perform customer due diligence has enhanced the efficiency, security and customer experience of the onboarding process. It has also enabled financial institutions to continue the onboarding of new clients during the COVID-19 pandemic, where there is greater demand for remote financial services delivery.

94. Additionally, *onboarding* tools that allow for quick CDD and client traits analysis (such as geolocation, credit checks, anti-fraud software and others) would also enrich the CDD and monitoring process and lead to a more accurate understanding of the nature of the business relationship, as well as its impact to the institutions.

95. The enhanced use of technologies, for client screening and matching, holds great potential to improve the compliance processes, as reliance on out of date and regionally irrelevant sanctions', PEP and other lists are acknowledged as an area in need of improvements (See Box 11). Such tools allow differentiation of similar names and other elements of identification, overcome language differences, identify cross-references with adverse media information and different databases. Natural

language processing and more advanced fuzzy matching tools could offer significant advantages to this function. Data harmonisation would also help to eliminate false positives and fraud attempts, as actors would begin relying on pooled information and varied verification systems.

96. Finally, digital solutions aimed at responding to customer due diligence challenges are believed to contribute the most to AML/CFT effectiveness when information sharing and data pooling is permitted and practiced, another illustration of the importance of overcoming data sharing barriers. Collaborative CDD was identified by respondents as a significant element of a more effective system and, therefore, one which policy-makers and supervisors should focus on developing, while finding adequate solutions to conciliate them with the need for the regulated entities to assume their responsibilities in accordance with a risk based approach.

Box 11. Machine learning for CDD purposes

Brazil

Brazil's Systemically Important Financial Institutions (SIFIs) are using machine learning in their monitoring and CDD/Employee/Partner processes in order to identify new ML/TF risks and increase the speed of analysis and the assertiveness of alerts.

To this end, they have specialized teams, data scientists and technological environment capable of supporting large volumes of data (ex.: SAS, Teradata, R-Studio, Foundry, Hadoop, Python, etc.).

Regarding monitoring processes and alerts

By using analytics tools and the integration of different databases, the SIFIs have created new scenarios, which resulted in a reduction of false positive alerts and in gains of efficiency in the analysis of alerts in general. It should be noted that many SIFIs are creating various thematic scenarios, the results of which have proven to be effective, especially those focused on situations involving the pandemic of COVID-19, such as the purchase of hospital equipment with public resources and the payment of emergency aid.

Based on a machine learning algorithm of the gradient boosting type, some SIFIs have created risk clusters, which allow for decision making by group rather than individual analysis, in order to score the likelihood that an alert will be reported to Financial Intelligence Unit (FIU).

Some SIFIs are also using the supervised clustering technique to specify rules for catching "outliers" in cash transactions while others are using univariate and bivariate exploratory analysis, feature analysis and feature engineering techniques to identify customers with transactions outside of their profile

A SIFI has developed a tool using analytics technologies to analyse the links between those involved in the alert, mapping relationships, risks and geographic information to support its analysis.

Regarding CDD processes

The SIFIs are using machine learning techniques to support their customer risk assessment, taking into account the various variables related to customer registration and financial transactions.

For instance, a SIFI is combining machine learning techniques (gradient boosting, random forest, voting classifier, among others) with logistic regression to select customers for reinforced due diligence. Other SIFI is developing tools to identify shell companies and implement integrated customer monitoring based on registration and financial information.

Outcomes

The SIFIs have already gained advantages in the results of their AML/CFT processes, such as:

- greater quality in the information obtained about their customers' behaviour, allowing for the generation of alerts from the customer´s point of view;
- greater assertiveness in generating alerts by identifying those greater risk to the supervised entities.;
- reduction of false positive alerts with the construction of more assertive rules by studying behaviours and patterns;
- greater effectiveness and efficiency in analysing alerts;
- quality improvement of reporting to FIU, providing more detail on the suspicious transactions;
- increase in the amount of suspicious transaction reports (STRs) to FIU as a consequence of the new scenarios and rules created;
- discovery of new ML/TF risks through increased data correlation, enabling better decision making;
- possibility of monitoring the customer as a whole from the registration and financial information available in the institutions of a conglomerate and external suppliers.

3.5. Application Programming Interfaces (APIs)

97. An API is a type of software which allows different applications to connect and communicate. APIs are also often used to provide payment services, for instance, in accepting donations over websites. Respondents to the Digital Transformation questionnaire mentioned APIs among the most used and relevant solutions to the identified money laundering and terrorist financing problems.

98. Their utility for AML/CFT lies in the ability to, for example, connect customer identification software with monitoring tools, or risk and threats identification tools with customer risk profiles in order to generate alerts or alter risk classifications as relevant. APIs allow this integration to happen much more quickly and with much larger datasets. This is particularly relevant as one of the most difficult challenges for many financial institutions is the integration of many different and often incompatible systems, including legacy technologies and specialised tools, created by different developers.

Box 12. Benefits of APIs

- Enhancing the interoperability between traditional banking data and moving away from siloed systems with fragmented frameworks.
- Increasing automation which can be reflected in the optimization of resources and output accuracy.
- Supplying an aggregated and normalized data feed, helping to build a more complete risk profile for new customers, for instance during the customer onboarding process.

99. API's also offer great value to the public sector by helping them access business registries and others, and providing the "agility to be modified for temporary monitoring purposes in response to unexpected shocks to the economy or more permanently in response to changes in financial system business models" [17].

Box 13. API in practice

The Hannibal Platform

The Tunisian FIU, CTAF, launched in January 2021 a Regtech named "Hannibal Platform" that permanently monitors the physical Cross-Border Transportation of currency. Hannibal platform is the fruit of the cooperation and coordination between the LEAs (Ministry of Interior and Customs), Banks, Post Office, Exchange Offices, under the oversight and the leadership of the Tunisian FIU.

Hannibal platform aims to understand, identify and assess the national risks of money laundering and terrorist financing related to the physical Cross-Border Transportation of currency.

17 (FSB, 2020[15])

This platform was designed using the Blockchain technology which is considered as one of the most important modern technologies in the field of data storage. This technology guarantees the transparency of the information and enhances its safety from any hacking attempts. The platform also relies on APIs that connect databases of the stakeholders (Ministry of Interior, Customs, Banks, Post Office, Exchange Offices and the Tunisian FIU).

The use of APIs enables the relevant authorities to obtain real-time data on the volume of importation of foreign currencies and all banking operations related to foreign currencies and a real-time data on foreign currencies' seizures by the LEAs.

Using that technology, it becomes possible for the relevant authorities to monitor the final destination of currencies exported or imported and declared to the Customs. It becomes also possible to carry out several intersections to get immediate warnings depending on the parameters being programmed and even to transform information into intelligence.

The Platform allows Tunisian authorities to take appropriate measures in order to mitigate the national risks of money laundering and terrorist financing related to the physical Cross-Border Transportation of currency.

Account Aggregators

IndiaStack, is a set of APIs that allows governments, businesses, start-ups and developers to utilise a unique digital infrastructure to solve India's problems towards presence less, paperless and cashless service delivery.

India Stack provides four distinct technology layers including a universal biometric digital identity, a single interface for all of the country's bank accounts, a secure way to share data and the ability of digital ID records to move freely, eliminating the need for paper collection and storage.

This infrastructure comprises of Aadhaar, eKYC, eSign, DigiLocker and UPI, tools that are facilitating orderly growth of open banking in the country.

The U.S. Social Security Administration's Consent Based Social Security Number Verification (CBSV)

The CBSV Service uses an API node that qualified financial institutions or their authorized service providers (permitted entities) can access to verify, with the individual's consent and for statutorily specified purposes, whether the person's name, SSN, and date of birth submitted by the permitted entity match that information in the SSA's records. CBSV returns a match verification of "yes" or "no." If SSA records show that the SSN holder is deceased, CBSV also returns a death indicator. CBSV does not verify an individual's identity.

At present, CBSV is typically used by companies that provide banking and mortgage services, process credit checks, provide background checks, satisfy licensing requirements, etc. CBSV has a one-time $5,000 initial enrolment fee, and a fee per-SSN verification transaction.

100. In addition to facilitating internal procedures, APIs facilitate communication between actors.

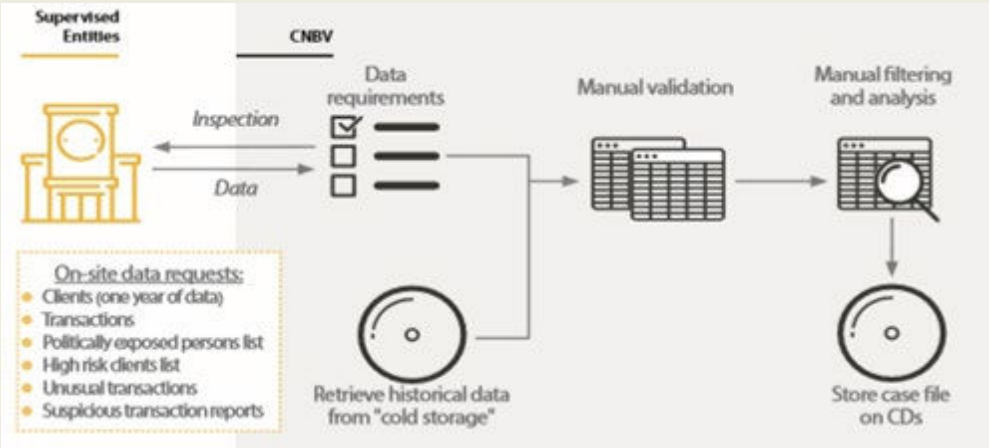
101. The use of APIs by supervisors, when combined with AI-driven analytics, could increase the efficiency of mandated reporting practices and the quality of the risk-based supervision. As shown in Box 14 below, this type of tool allows supervisors to process historical data in tandem with onsite inspections data and contextual factors and generate automated reports for consideration and defining action.

102. This automated analysis offers the possibility to provide supervised entities with more immediate and detailed feedback of the supervisory process and expectations.

Box 14. Mexico

Inefficiencies in AML data architecture combined with many financial institutions categorized as high-medium risk results in *inadequacies in drawing deep insights* from data informing onsite visits or otherwise as well as *delayed and unproductive auditing.*

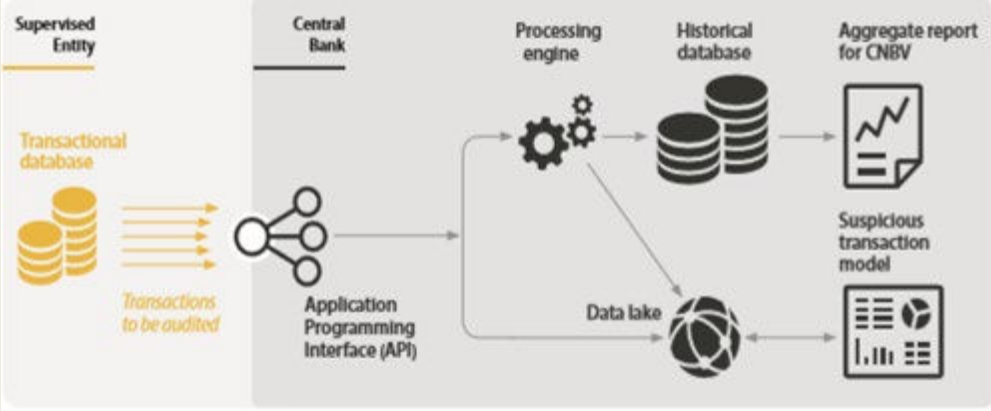
The starting point:



SupTech Innovation Solution:

An *API*-based AML data architecture and *AI-driven analytics* tool, which includes: a Centralized platform to generate standardized, automated requests to supervised entities with raw data received through push or pull submission stored in a data lake. An API to establish secure, direct line of machine-to-machine data transmission feeding the data into a processing engine instantly running validations tests verifying quality, content and structure of reports and funnelling processed data into the data lake creating a consolidated, single and access-controlled data architecture. AI-driven analytics that detects suspicious transactions using predictive analysis and ML techniques (clustering, neural networks, logistic regression, random forests) and recommend AML

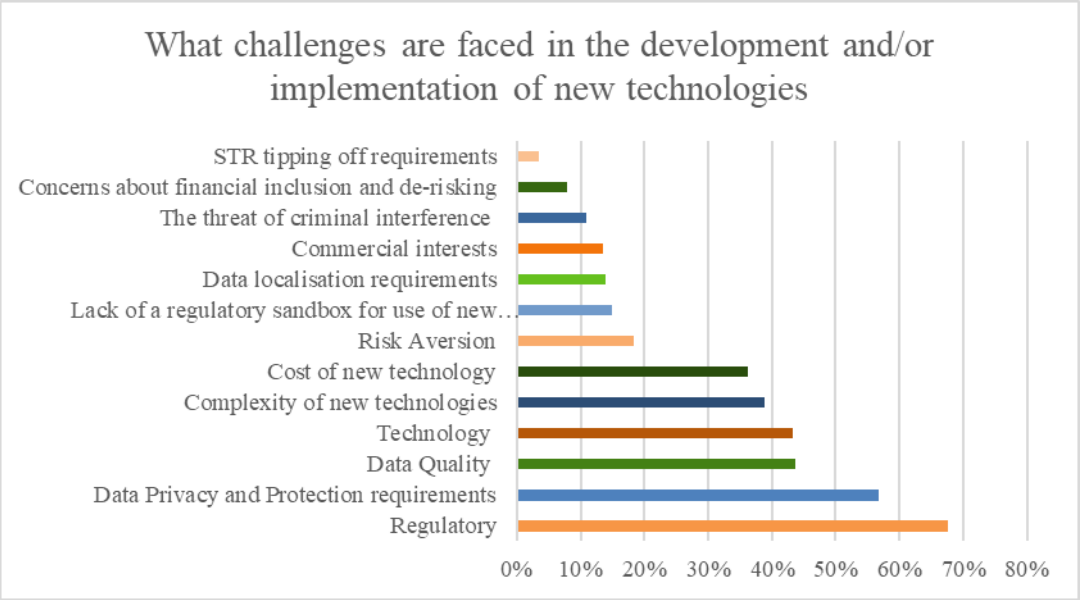
alerts using ML based on FIs underlying risks exposures. Dashboards and watchlist tracker provide a view of the AML risk landscape. In a second phase the toll will include an AI-driven analytics tool that detects suspicious transactions using predictive analysis and ML techniques (clustering, neural networks, logistic regression, random forests) and recommend AML alerts using ML based on FIs underlying risks exposures.



4. The Challenges of Implementation of New Technologies for AML/CFT

103. The adoption and implementation of new technologies to the AML/CFT frameworks is not without challenges. Core challenges are either regulatory or operational.[18]

Figure 3. Challenges in the Development and/or Implementation of New Technologies



4.1. Regulatory challenges

104. Data collected for this report suggest that there is a need for clear support from FATF and national competent authorities for innovation in AML/CFT. A few experts expressed a desire to have "technology-active supervisors" – supervisors willing to engage with technology developers - rather than technology neutral approaches. Respondents believe that a lack of express support by competent authorities and FATF has led to diminished interest, investment and trust in new technologies, despite their potential.

105. The interpretability and explainability[19] of new technologies to supervisors is key to securing support for these tools. Regulated entities must be able to explain, and remain responsible for, the principles and technical details of the innovative solutions before deploying these new technologies. Supervisors must be able to understand the models used by AI tools in order to determine their accuracy and their relevance to the identified risks. However, a few respondents stated that most supervisors do not have the expertise or resources that would allow them to understand and adequately supervise new technologies.

18 As confirmed by (Richard Grint et al, 2017[14])

19 For more on this see (EBA, 2020[17])

106. Respondents also mentioned that even the most technologically-literate supervisors are often slow to adjust regulatory practices. Indeed, while some jurisdictions already promote the adoption of new technologies through innovation events and other forms of regulatory support (see Box 15), these efforts do not always translate into supervisory acceptance of new procedures and compliance practices.

Box 15. Levering public infrastructure to facilitate digital CDD-procedures

The Danish FSA has recently issued a public consultation on technological initiatives that can support companies, who are subject to AML/CFT regulations in their efforts against financial crime, "project AML/TEK". The aim is to stimulate discussion on this very important topic and to gain insights to ensure an enlightened political discussion on the way forward.

The analysis presents pros and cons of seven initiatives that have the potential to strengthen the first line of defence by leveraging technology. The analysis generally reflect the highly digitised nature of the Danish society, but also raises issues of universal interest on the trade-offs involved, in particular between fighting financial crime and data protection and privacy.

The analysis seeks to provide a baseline for further discussion. Most of the initiatives come with legal implications for obliged entities and for customers and also raise questions concerning the legal basis for accessing and sharing the data in question. Three of these initiatives can support further digitalisation of CDD-procedures:

Increased access to relevant public registers

A central barrier for obliged entities to digitalise their CDD procedures is the absence of verified digital customer information. As Danish authorities have several registers with relevant customer information, the analysis examines granting increased access to these registers. The analysis looks at access to data in several registers, for example data held by the Danish Business Authority, the Danish Tax Agency, the passport and driving licence registers, the Danish Immigration Service's registers and so on.

Quality assurance of data in the Danish Business Register

Data available in the Danish Business Register is provided by the obliged entities themselves. Hence although most company master data is accessible through an API and is subject to a comprehensive control environment, identification of all faulty or misleading registrations is not certain, which compromises the applicability of the data for CDD purposes. The analysis thus proposes to look into whether it is possible to establish a mechanism whereby lawyers and approved auditors can verify the registered data.

PEP-screening solution

Screening of PEPs and their relationships is a resource-heavy manual process for obliged entities and requires them to obtain personal data about their customers. In Denmark, such relationships could to a large extend be mapped through public registers, although this raises serious data protection concerns. The analysis looks into establishing a public PEP-screening solution which could improve the quality and reduce the cost of PEP-screening through increased digitisation, while at the same time minimising the collection of personal information.

107. The use of new technologies for AML/CFT can only truly become effective if systems are based on standardised data that is easier for technology developers to integrate into their tools, easy to understand and explain to non-experts, and easy to communicate to counterparts and competent authorities when needed. This issue also shows the importance of public authorities, particularly FIUs, providing reliable feedback to reporting entities on suspicious activity and ML cases that can be used for training purposes. Training a machine learning system based on real cases which have been positively verified as involving ML or TF - if these were available - would offer a significantly better hit rate than training an AI to replicate the decisions of a human compliance officer about whether the appropriate suspicion threshold is met. Furthermore, the ability of FIU's, and other competent authorities, to offer feedback on which reports are of most utility, through automated processes, would also help FI's train and inform internal compliance teams and systems.

108. Data harmonisation (or lack thereof) was also mentioned as an additional obstacle, because the costs of investing in new technologies and expertise increase exponentially if these systems required fine-tuning and adjustment to different jurisdictional requirements and formats. Data harmonisation therefore offers significant advantages to the creation of an enabling environment for the implementation of new technologies as it allows actors to converge in goals, for example, a common transaction monitoring, providing feedback to private sector and risk assessments. Ensuring data quality - a concern shared by 45% of respondents to the digital transformation questionnaire - is seen as an obstacle to the adoption of AML/CFT technology-based solutions.

109. The real or perceived issues of interpretability have also led to constraints in the ability to build trustworthy relationships between technology providers and users, and a lack of trust that data processed through new technologies can be robust. Nevertheless, an increasing number of actors are registering data on large scale and this upscaling of operations has meant a greater ability to match different sets of complex data.

110. The role of third parties as providers of new technologies was deemed to be sufficiently clear by 60% of respondents to the digital transformation questionnaire but additional guidance on how to interpret current regulations in the digital era was requested by private sector respondents.

111. Additional clarification was called for, by the private sector, as regards the issue of accountability, transparency and the supervision of entities using new

technologies. As the adoption of technologies in this space picks up pace, supervisors should reflect on what kind of tools regulated entities are adopting and whether providers (vendors) of these tools should fall under additional scrutiny, for example, as service providers to regulated entities or via separate regulation and supervision. Authorities might also consider whether innovative AML/CFT technology used by regulated entities and/or by regulatory authorities can be more effectively leveraged by new forms of collaboration, for example, public-private partnerships or expanded access for regulated entities to government data-bases. However, the use of innovative solutions should not call into question the ultimate responsibility lying with regulated entities.

112. Whilst the increased uptake of new technologies will likely enhance supervisory practices, respondents mentioned a balance must be struck between the importance of integrating technologies and "*the importance of retaining a forward-looking human based* supervisory *process*."[20] With a view to adopting this approach, the majority of available tools still include human input and review as a key component and evidence that these tools are not replacements of current systems, but their enhancement.[21]

113. Human input and capacity building were identified as continuing to have an essential role in supporting the adoption of new technologies for AML/CFT, in particular regarding elements that technology still cannot overcome, regional inequalities or expertise on emerging issues. This report has identified numerous instances of successful collaboration for AML/CFT purposes which were technology aided but relied essentially on dialogue and commitment between actors to achieve success. These collaborative approaches between public and private actors, for example, for the purposes of identifying ML/TF red-flags were able to demonstrate the immediate benefits of using technology to address specific challenges whilst not being completely dependent on these tools for effectiveness.[22]

114. Similarly, systems based on state-issued digital identity tools appear to allow for greater success in the uptake of digital ID systems and collaborative platforms compared to systems that rely on the collection of data from multiple sources. Data validation may be one aspect were *human* authority will continue to take precedence. Furthermore, as the use of new technologies becomes more widespread, actors must also consider the degree to which *machine error* becomes, or may not be, acceptable.

115. The increased effectiveness of AML/CFT is also limited, among other non-AML/CFT related reasons, by the inability of regulated entities to share information with their

---

20 (FSB, 2020[15]), pp 32.

21 For more on relevant developments in the field of suptech and its links to regulatory reporting please see Crisanto et al, From data reporting to data-sharing: how far can suptech and other innovations challenge the status quo of regulatory reporting?, (BIS, 2020[18])

22 See, for example, the COMCRIM project to combat crimes that undermine the rule of law such as human trafficking, money laundering and corruption in a smart and comprehensive manner, in a financial public-private partnership and through artificial intelligence. Available at: www.uva.nl/en/about-the-uva/organisation/faculties/amsterdam-law-school/research/research-themes/labour-exploitation-human-trafficking/labour-exploitation-and-human-trafficking.html. See also the work of a non-profit network of expert, The Knoble, working towards preventing financial crime through collaborative and tech-based approaches. Available at: www.theknoble.com/

counterparts and across borders. Ultimately, to fully understand the nature and risk of suspicious transactions actors require access to their full pathway which is often beyond borders or held by other entities. New technologies may offer significant value to overcoming this challenge as discussed in greater depth by the FATF Stocktake on Data Pooling, Collaborative Analysis and Data Protection report.

116. Finally, the issue of security and protection from criminal interference did not come up high on the list of identified challenges in private sector responses, though it may be more significant from a public policy and law enforcement perspective. Nonetheless, there is a growing number of criminal cases associated with the use of technologies, for example, related to identity fraud or criminal operations that use "money mules'' which should be taken into account in assessing the impact of new technologies in regulated entities' operations and criminal activity in general.

4.2. Operational Challenges

117. Operational challenges mostly relate to to adapting practices to new and sometimes untested systems, or technology solutions. Issues related to the costs of new technologies, the ability of actors to understand and train staff to implement them, as well as the replacement of legacy systems with the new tools, were among the core issues raised by respondents.

118. Despite the wide acknowledgement of advantages, the adoption of new technologies by supervisors is lagging behind the private sector levels. Respondents stress the need for supervisors to update their own systems and supervisory strategies to be able to better interpret and supervise AML/CFT in the digital age.

119. Supervisors identified the costs associated with the replacement of legacy systems, the availability of quality reported AML/CFT data, and the availability of specialised resources and skilled or expert staff as their greatest difficulties.

120. Procurement processes for updating legacy systems, for example, are overly complex, lengthy and often not targeted at the right actors. A few respondents stated public procurement processes for SupTech are often not interesting or visible to technology providers because they require knowledge of public procurement processes and specific governance goals, which technology developers' lack. Moreover, the kind of technology sought by the public sector is often either out of date by the time it gets to the procurement stage, or is called-for in a way that is overly prescriptive and not appealing to technology providers (i.e. calls for exclusivity). Such practises deter developers from producing off-the-shelf products intended for supervisors.

121. Challenges in this regard include reluctance to invest in new technologies that may: be difficult to integrate with legacy systems and/or beyond the regulated entity's technical capacity to use appropriately and effectively; become out-dated and require additional investment in newer solutions; not meet regulatory expectations or fail to satisfy a particular examiner, who may lack capacity to evaluate the solution's effectiveness or is uncomfortable with innovative solutions for other reasons; present risks, including potential privacy violations and AML/CFT compliance failures. Smaller financial institutions in particular often lack internal capacity or confidence to evaluate the effectiveness of a given innovative solution among a large and growing range of competing vendors and products, to determine if it is appropriate for the institution's risk profile, customer base, and business activities, or to implement models and manage model risk.

122. Generally, respondents agreed that some supervisors are not as engaged as the private sector, with the technology sector as regards being aware of new trends and emerging digital solutions. Their lack of specialist skills (and resources) and knowledge increases the challenge of interpretability of new technologies and, for the most part, limits of their potential for AML/CFT effectiveness.

123. Some respondents also mentioned that as a result of the lack of harmonisation, technology use at scale might be impossible. This could potentially prevent innovation from reaching cost-effectiveness and hamper its development. Using big data most efficiently, for instance, requires that it be available across multiple entities. Without this scalability, some technological tools might not be financially feasible.

124. The inability to develop technologies to scale moreover exacerbates the gaps between the uptake of large and smaller entities, and different regions. Respondents agreed a wider implementation of technology will only be possible if there are more significant incentives, either mandated use or a greater trust environment, that support investment and justify reform of smaller financial operations and other non-financial obliged entities.

125. New technologies have improved data quality but will continue to rely on human input and manual review. Machine learning tools rely on existing systems and their manual updating thus possibly generating instances where "bad data" is inputted and has a negative impact on the models adopted. This includes the data which a machine learning system is trained on, e.g. to learn to identify suspicious transactions. If the training data includes false positives or other errors, these errors will be "trained-in" to the machine learning system, although some margin for error will still be needed for instances of human bias or unidentified errors.

126. The automation of the initial data input through natural language processing tools could also improve data quality by minimising the errors of customers or staff registering the data.

127. Finally, consumer appetite for new technologies in financial services was identified as one of the least significant drivers of the adoption of new technologies. Moving forward the role and consumer perspective may, nonetheless become increasingly relevant, as CDD and other individual focused digital solutions become more prominent.

128. As actors overcome the regulatory and operational challenges identified, it may be worth considering the customer response to traditional CDD and monitoring procedures, but also the new applicable approaches and the ways in which these impact data protection and privacy. Consumers may not impact the development of these technologies, but are nevertheless affected by tools which change the customer experience of interacting with a regulated entity. While the use of new technologies for AML/CFT could also favour the customer experience, there are risks and unintended consequences to digitalisation which must be taken into account in the adoption and implementation of these tools.

129. Among the most frequently cited risks of digitalisation is the abuse of the system by criminals and its contribution to increasing the vulnerability and financial exclusion of certain segments of society i.e. the elderly, rural or distant (less connected or remote) communities.

Box 16. Overcoming operational challenges

The Hong Kong Monetary Authority (HKMA) has taken a number of steps to identify the common operational challenges encountered by banks when adopting new technologies, and implemented a series of activities to assist banks in overcoming these challenges, commencing with an AML/CFT Regtech Forum in November 2019. Conversations took place with about 40 banks throughout 2020 across three working groups according to their maturities in technologies adoption—to better understand how Regtech was being approached as a means to enhance AML/CFT processes.

The effort culminated in January 2021 with the HKMA sharing hands-on experience from banks that have implemented AML/CFT Regtech, in the form of a report "*AML/CFT Regtech: Case Studies and Insights*" (Hong Kong Monetary Authority/Deloitte, 2021[15]). The report seeks to build awareness and lower the real and perceived barriers to AML/CFT Regtech adoption by sharing case studies and illustrating different approaches adopted (e.g. use-case-led versus solution-led approach). It also provides early adopters' insights, technology spotlights and guidance on addressing key operational challenges (such as data and process readiness, stakeholder buy-in and executive support, and considerations when working with third party vendors). The report is constructed so that banks at different adoption maturity levels can navigate to a technology application they are interested in or a challenge which resonates with them. Follow-up activities targeting different maturity groups, for example through industry sharing and interactive lab sessions are in progress.

4.3. Unintended Consequences and Potential for Abuse

130. The use of innovative technology in the financial sector brings with it not only significant and potentially transformative benefits, but also risks of unintended consequences, potential conflict with competing objectives, such as privacy, inclusion, equitable outcomes, and vulnerability to witting abuse. While AI has become an essential tool across a broad range of industries, including financial services, health care, retail, and manufacturing, where it has improved efficiency, reduced costs, and accelerated research and development, its growing use has raised a host of ethical and legal concerns that have generated widespread calls and numerous workstreams to develop appropriate government and private sector standards and safeguards.

131. AI/ML solutions vary greatly in both technology and use and may present significant risks. Potential lack of explainability and transparency can undermine the ability to assess an AI/ML solution's accuracy in identifying suspicious transactions and other illicit activity, so that its effectiveness as an AML/CFT compliance tool cannot be established. In addition, although algorithmic decision-making may seem to offer an objective way of overcoming human subjectivity and

prejudice, researchers are discovering that many AI algorithms replicate program developers' conscious and unconscious biases and apply them at scale to unfairly target as suspicious the financial activities of certain types of individuals or entities, or produce risk profiles and decisions that deny them access to certain financial products and services.

132. Similarly, although trustworthy digital identity solutions can significantly strengthen customer identification/verification at onboarding and support other CDD measures, as well as help combat fraud and cybercrime and facilitate financial inclusion, digital identity solutions that do not provide adequate risk-based technical assurance and appropriate governance present operational risks and potential unintended consequences. They are also open to deliberate abuse.

133. When adopted without regard to the risk based approach or proportionality, digital identification solutions may add to the exclusion of underserved communities. For example, asylum seekers may not be able to provide initial documentation that providers of digital ID sometimes require in order to generate such a digital ID. There are further potential unintended consequences of digital ID tools to consider, in particular on the challenges related to a potential disclosure of personal information.

134. When used for financial services, the amount of personal data required from costumers is elevated since a high level of assurance regarding the real identity of individuals for the purpose of CDD and AML regulation is necessary. However, to properly implement the financial inclusion objective, Digital ID tools should be inclusive in their design and operation.[23]

135. The FATF requires "reliable and independent digital source documents, data or information". (FATF, 2020[8]) This means that the digital ID tools used to conduct CDD must rely upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results.

136. To this end, legal, procedural and social barriers in identification systems should be identified and mitigated, with special attention to underserved people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons). (World Bank, 2021[16])

137. Operational risks and risk mitigants, including unintended exclusion and privacy risks, are discussed in Section V of the FATF's Guidance on Digital Identity[24]. Stakeholders are encouraged to consult this document. In addition, the World Bank's updated Principles On Identification For Sustainable Development: Toward The Digital Age (World Bank, 2021[16]) provides an essential set of principles to guide the design, governance, and use of digital identity systems, with the aim of helping ensure that they are inclusive, consent-based, protect privacy and other rights, and are fair and accountable.

23 Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data convention 108. See (Walshe, 2020[20])

24 (FATF, 2020[8]) pp. 35-45.

Box 17. Challenges posed by biometrics data

Biometric digital identity tools can raise potential conflicts with human rights, mostly in relation to the rights to privacy (e.g. UDHR, Article 12) and freedom from discrimination (e.g. UDHR, Article 7). This potential conflict is reflected in some laws and conventions, the modernised Council of Europe Convention 108 (108+), and the EU General Data Protection (GDPR) Regulation, which considers 'biometric data' as a special category of data requiring a higher level of protection in order to safeguard individuals against adverse effects of its use. Concerns have also been raised that the broad scope of biometrics technology and its rapid development and use for multiple purposes may put key human rights at risk. (CoE, 2011[17])

If digital identity solutions were biometrically-based and were made mandatory, they would have the potential to become a pervasive means of identification, tracking or control, negatively impacting the right to privacy.

Biometric information collected by private parties should therefore be recognised as protected information, subject to the legal standards required for such data under international legal instruments, and its use limited under the proportionality and necessity principles.

4.4. Assessing AML/CFT effectiveness of technology solutions and how to address residual risks

138. As actors start to deploy new technologies after overcoming the challenges identified above, it is important for regulated entities to continually examine the effectiveness of these new technologies to detect and combat ML/TF risks. By putting in place measurements of effectiveness, regulated entities will be encouraged to be more outcome oriented, and also ensure that the adoption of new technologies is fit for purpose and continue to perform adequately over their life cycle.

139. These effectiveness measurements will also serve as a feedback loop for both public and private sector to re-calibrate their technology-based solutions, if they do not fulfil the intended purpose. At the same time, having clear measurements will help to aid supervisors in their assessment of new technologies employed by the regulated entities.

140. Further, all actors should assess whether there are residual risks that may arise with the use of new technologies, or where there are key human elements which cannot be fully replaced by new technologies. It is essential to ensure that there is no over-reliance on new technologies, and where residual risks are identified, regulated entities should demonstrate awareness of these risks and the ability to manage or respond to these when needed.

141. Nonetheless, it has been identified to be challenging to develop such effectiveness indicators and to determine the acceptable level of effectiveness or residual risks and there is scope for sharing of best practices and/or guidance.

5. Creating an enabling environment for the use of new technologies in AML/CFT

142. Respondents agreed that FATF and competent authorities need to do more to overcome the existing regulatory and operational challenges to the implementation of new technologies for AML/CFT. However, it is important to recall the unintended consequences of removing certain frictions present in the system.[25] For example, faster execution of transactions means there is less time to identify criminal activity and increases the pressure on the systems trying to detect and prevent financial crimes.

143. The opportunities and challenges of using new technologies for AML/CFT may depend more on regulatory and policy responses than additional technological development. The case for the use of new technologies is valid for public and private sectors alike as it enhances overall AML/CFT capabilities, the ability to collect and better visualise data, monitor criminal activity whilst simultaneously making a more efficient use of resources.[26]

144. Different ways to promote the adoption of SupTech and RegTech technologies have been discussed by others (BIS, 2019[18]) stressing the importance of senior management buy-in and the need to secure interpretability and explainability. The ability of regulated entities to demonstrate to their supervisors, and internally, the benefits of new technologies is key to their adequate adoption and supervision. Going forward, the focus should be on using technology to address identified challenges and demonstrate progress in achieving AML/CFT effectiveness.

145. Other examples of supervisory collaboration with industry confirming efforts to overcome explainability issues are available, namely guidance to industry on how to resolve the "black box" model. (MAS, 2018[18])

146. Some jurisdictions, as illustrated in Box 18, and mostly large financial sector entities have already begun adopting and using new technologies as part of regular compliance efforts, but emphasise that its true added value will only be achieved when these are adopted in scale and by the majority of actors around the globe.

Box 18. Personal Account on the Rosfinmonitoring website

Rosfinmonitoring (Russian Federation) actively develops a Personal Account (PA) on its website as a mechanism for communication with the private sector. PA performs as IT-solution that combines SupTech and RegTech functions. Initially PA was designed to file STRs and circulating the list of designated persons.

In 2018 after the "pilot" mode was over, PA became mandatory for all reporting entities. Currently it is 80 thousand reporting entities

25 (WEF, 2020[24]), pp 21

26 Idem. Pp.8

including 60 thousand DNFBPs who use PA regularly. It has proven to be an effective risk mitigation tool for private sector.

PA permits conveying information generated in an automated remote monitoring system (ARMS) used by Rosfinmonitoring to calculate risk assessment for supervisory goals. Each reporting entity can receive information on deficiencies in its activities concerning all aspects of internal control (filing STRs, risk management, use of list of designated persons, etc.). It allows organizations to mitigate deficiencies remotely.

This function is especially relevant for DNFBP sector. Annually about 2 thousand DNFBPs succeed in mitigating deficiencies as a result of using the information received from PA.

PA works as a feedback mechanism on STR. It provides financial institutions with the information flow quality index, which includes number of criteria defining effectiveness of STR reporting by obliged entities.

PA allows FIU to exchange information on ML/TF risks and typologies, disseminate results of national and sectoral risk assessments.

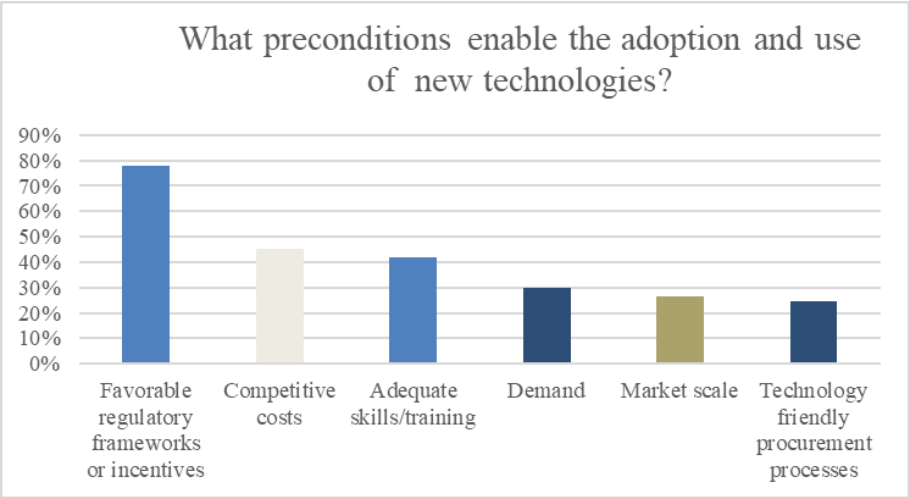
PA function aims to increase the level of awareness of legislative requirements amid private sector. Distance e-learning plays a significant role in this process.

There is a number of training courses developed by International Training and Methodology Centre of Financial Monitoring and placed in Personal Account. Soon specific courses on PEPs and beneficial owners risk management are going to be introduced.

In 2018, PA for supervisors was launched. It contributes to operational risk-exchange between Rosfinmonitoring and supervisory bodies.

147. A favourable regulatory environment, competitive costs, expertise (training) and scale were identified as key preconditions to the adoption of new technologies as evidenced in Figure 4.

Figure 4. What Preconditions Enable the Adoption and Use of New Technologies?



148. Supervisors should take a proactive approach to technology. This will promote the preconditions that enable adoption and use of new technologies and assist members in a more effective implementation of AML/CFT Standards.

5.1. Technologically-Active Supervisors[27]

149. If supervisors and FATF show more active support for new technologies it would help respond to the outstanding risk and trust concerns expressed by regulated entities. Support for new technologies is already taking place in many jurisdictions in the form of tech-sprints, accelerators, innovation hubs, and other collaborative initiatives where the private sector is able to develop, present, and test its tools, as well as receive feedback on their applicability to the AML/CFT frameworks (see Box 19 below). Neither the FATF nor individual supervisors should take positions on individual technologies or providers. The responsibility for compliance with AML/CFT requirements remains with the regulated entities. Rather, the role of the FATF and individual national authorities should be to enable innovation and new approaches allowing the market to support trustworthy and proven technologies within the bounds of appropriate regulation and supervision and with respect for public policy objectives set by national governments.

150. Whilst these opportunities are noteworthy (*additional examples in Annex C*), respondents believe that collaboration in this area must go beyond specific events and take the form of ongoing exchanges and cooperation between supervisors and supervised entities. Overcoming the fear of regulatory penalties or sanctions requires a more constant interaction than that experienced by respondents, for example in the form of a full regulatory strategy reform that adjusts to the digital era or specific guidance for implementation as suggested in Box 20.[28]

151. This perception is supported by a report submitted to the European Commission suggesting "Thirty Recommendations on Regulation, Innovation and Finance" (EC,

27 Not to be confused with endorsing specific technologies or digital solutions. FATF and supervisors should remain technology neutral.

28 See also the HKMA experience as an example of best practice. (HKMA, 2020[26])

2019[19]) many of which are corroborated by the findings of this report. Among them, the need to: clarify the explainability and interpretability of AI and associated technologies, promote the use of digital ID and remove default paper requirements, promote the use of technology-driven financial services, and develop and implement measures to support RegTech and SupTech.

Box 19. Innovation hubs, Tech-sprint and Sandbox examples

BAFIN – Germany

BaFin initiated in 2020 a project called "TechBridge" which established new institutionalized exchange formats for innovators including on AML/CTF issues. The core component involved confidential individual workshops attended by an innovator and a group of selected BaFin experts.

The workshops can take place as early as the research and development phase of the innovation tool has begun. First and foremost, the new tools must potentially raise new supervisory and/or regulatory issues.

Further selection criteria include whether the new tools could have a major impact on the financial market and potentially entail high risks.

Financial Conduct Authority - UK

The FCA has taken a number of steps to encourage the responsible use of new technologies to meet AML/CFT obligations:

The FCA regulatory sandbox allows regulated entities to test innovative products, services and business models in a live market environment, while ensuring that appropriate safeguards are in place. It opened for applications from June 2016 and there have been six complete cohorts of the sandbox. Across all of these cohorts regulated entities have tested AML innovative solutions around both transaction monitoring and identity verification. Regulated entities work closely with the sandbox to ensure that risks are identified and appropriately mitigated. The main interventions are providing early steers on the application of AML regulation; enabling regulated entities to iterate their business models; and guiding regulated entities through regulatory processes critical to launching a new business, service or product.

In July 2017 the FCA published a report it had commissioned from PA Consulting about how new technologies are being used to streamline AML compliance.

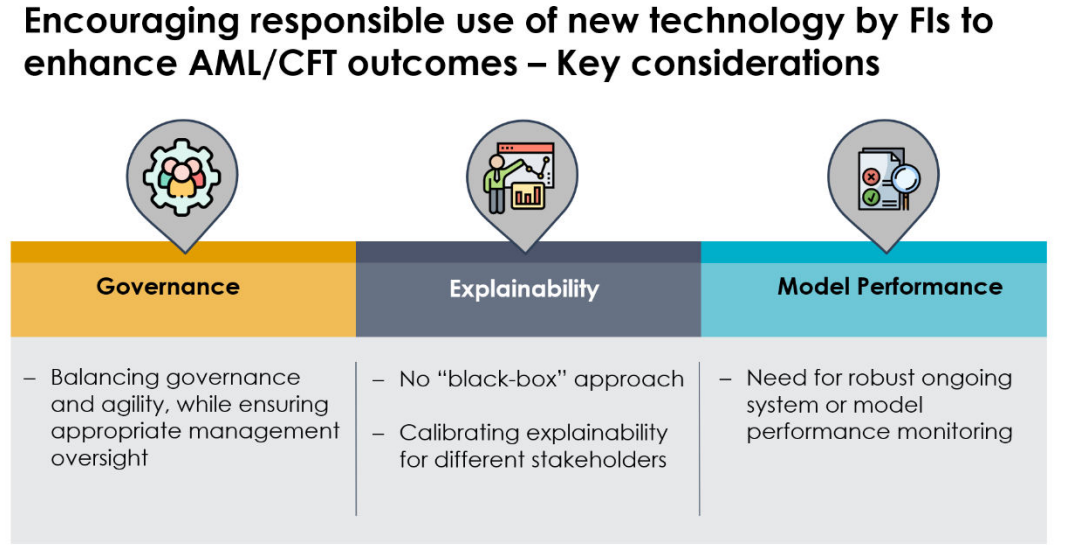
Giving clear messages in speeches about the opportunities technology offer to improve AML compliance and the FCA's encouragement for the experimentation and deployment of such innovations. Megan Butler, Executive Director of Supervision – Investment, Wholesale and Specialists at the FCA spoke about the FCA's view that used to the right ends such technologies can be gamechangers in the fight against financial crime entitled 'turning technology against financial crime'.

Encouraging interaction and knowledge-sharing between Supervisors and RegTech providers on the use of technologies by regulated regulated entities. Holding 'TechFairs' where existing and potential market participants demonstrate solutions being developed and employed in the market to allow Supervisors to better understand advantages as well as raise concerns. Actively encouraging the discussion of how emerging technologies not currently or widely utilised within financial services could provide benefit, for example the 2019 TechSprint to explore the potential for PETs to combat financial crime and money laundering, thus demonstrating institutional commitment to the adoption of new solutions.

Sweden's Financial Supervisory Authority

Finansinspektionen established an Innovation Centre in 2018 with the purpose of offering guidance, providing information and maintaining an ongoing dialogue with regulated entities and start-ups that offer innovative products and services within the financial sector. The Innovation Centre also arranges seminars and information gatherings and participates in external events relating to innovation in the financial sector. One current example is participating in roundtable discussions with different service providers from the private sector in the rapidly evolving area of virtual assets. Recent topics for discussion at such events have been new relevant regulation and the EBA's revised guidelines regarding de-risking and risk mitigating measures within the AML/CFT area. Finansinspektionen takes the position that financial regulation should not obstruct development and innovation in the financial sector, provided that the primary assignments by Finansinspektionen are not disregarded. Finansinspektionen takes a positive view on innovation that strengthens consumer protection while at the same time contributing to financial stability, well-functioning markets and sustainable development.

Box 20. Monetary Authority of Singapore



Together with the financial industry, the Monetary Authority of Singapore (MAS) has developed a set of principles to promote Fairness, Ethics, Accountability and Transparency (FEAT) in the use of artificial intelligence (AI) and data analytics in the financial sector. This set of principles provides guidance to financial institutions (FIs) on the responsible use of AI and data analytics, to strengthen internal governance around data management and use.

Specific to the area of AML/CFT, MAS has been actively working with the industry to address key challenges in the implementation of AML/CFT data analytics. In 2019, MAS collaborated with FIs through Singapore's AML/CFT Industry Partnership (ACIP) to exchange perspectives on data analytics issues. During the workshop, MAS and the industry landed on three key principles to encourage the responsible adoption of new technologies – namely governance, model explainability and model performance. There was consensus that there should be no compromise on robust governance, as FIs adopt more innovative approaches in tackling financial crime. Explainability should also be a design priority for the system to be effective, and should be considered at the onset of system development.

152. Innovative approaches and collaborative supervision has also been identified in the most emerging areas of new technologies. Distributed Ledger Technology has been identified as having particular importance in the supervision of virtual assets. A number of initiatives have developed globally, with a view to supporting the development of these technologies and create an enabling environment which allows for stakeholder dialogue and overcoming some of the challenges associated with innovation.

153. Unlike transactions through conventional intermediaries such as banks, transactions of virtual assets (VA) based on DLT are often conducted without the

use or involvement of intermediaries and other obliged entities, and they face obstacles to achieve regulatory objectives, especially those related to AML/CFT, due to the difficulties in tracing and monitoring transactions that may derive from its unique nature. As virtual assets become more widespread, the risk mitigation through the use of intermediaries may become challenging over the medium to long term.

154. Therefore, in the space of VA transactions and blockchain based finance, one promising direction is to explore the ways to ensure development of protocol and computer codes that facilitate AML/CFT compliance while maintaining benefits of innovation (Yuta Takanashi et. al, 2020[20]). As the developers, protocol designers and third party providers are not explicitly subject to AML/CFT obligations under the FATF Recommendations, the FATF should consider whether additional discussion is needed with other stakeholders, for example, as regards the role of technology providers, and growing use of blockchain in finance in AML/CFT, to ensure the relevancy and effectiveness of FATF standards in the mid-long term.

155. Finally, the FATF has also identified *Suggested Actions to Support the Use of Technology in AML/CFT* (see Annex B) that advance the 2017 San Jose Principle to *pursue* positive *and* responsible *innovation*. These Actions note that new technologies for AML/CFT must be developed and implemented in a way that reflects threats as well as opportunities, ensuring that their use is compatible with international standards of data protection and privacy, and cybersecurity.

Box 21. Supervisors and DLT

JFSA – Japan

The Blockchain Governance Initiative Network "BGIN" initiative was launched in March 2020 and JFSA has proactively contributed to it. This initiative has been tackling the challenges of the decentralised financial system underpinned by blockchain technologies by adopting a so-called multi-stakeholder approach. The importance of enhancing multi-stakeholder dialogue was advocated by the FSB (FSB, 2019[21]) and welcomed by G20 under Japanese Presidency in 2019 (G20, 2019[22]). This concept aims to form a common understanding on issues stakeholders are facing through dialogue on an equal footing among various stakeholders such as regulators, technology developers, obliged entities, academia, etc., given the limitation of the conventional regulatory framework: unilateral communication from regulators to obligated entities.

BGIN explains its objectives (BGIN, n.d.[23]) as to "take a leading role to design healthy governance where stakeholders develop a common understanding, enhance dialogue, and work together and make a real positive impact for the ecosphere and society at large" and tentatively focuses on:

- creating an open, global and neutral platform for multi-stakeholder dialogue,

- developing a common language and understandings among stakeholders with diverse perspectives, and
- building academic anchors through continuous provision of trustable documents and codes based on an open source-style approach.

BGIN deals with various issues relevant to FATF including, for example, identifying potential regulatory approaches of AML/CFT in DeFi (decentralized finance) taking into consideration emerging technologies and market developments. It may be beneficial for FATF and its members to get involved in its activities as a place to enhance dialogue with various stakeholders including those who develop technologies, to whom regulatory authorities usually face challenges to access. Such continuing engagement with stakeholders, as indicated in the FSB report, would eventually ensure the compliance on AML/CFT while avoiding stifling the innovation and its enabling environments.

5.2. Concluding remarks

156. This report offers a high-level overview of the opportunities and challenges of new technologies for AML/CFT providing, where possible, examples of existing best practises and/or specific challenges. The findings of this report are not all encompassing and there is room for improvement in the relationship between FATF standards and digital transformation.

157. Technological innovation offers great potential to the effectiveness of AML/CFT. However, it may also lead to increased financial exclusion of certain segments of society – elderly, rural communities etc., as well as create challenges to society, in particular in terms of human rights, democracy and rule of law. The FATF is mindful that further challenges may emerge as a result of irresponsible or misguided support for, and reliance on, new technologies by actors.

158. FATF encourages jurisdictions to work together and with private sector actors to consider a holistic approach to new technologies, taking into account its potential as well as its limitations.

Annexes

- Annex A – Glossary
- Annex B - Suggested Actions to Support the Use of Technology in AML/CFT
- Annex C – SupTech case-studies
- Annex D - Additional RegTech case studies for the uses of new technologies for AML/CFT by the private sector

Annex A: Glossary

- **Advanced Analytics**: Advanced analytics refers to the autonomous or semi-autonomous examination of data or content, using sophisticated techniques and digital tools, typically beyond those of traditional business intelligence, to discover deeper insights, make predictions, or generate recommendations. Advanced analytic techniques include those such as data/text mining, machine learning, pattern matching, forecasting, visualisation, semantic analysis, sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, simulation, complex event processing, neural networks. Advanced analytics typically rely on the use of big data.
- **Application:** An application is computer software designed to help a user perform specific tasks.
- **Application Programming Interface (API):** An API is a set of definitions and protocols for building and integrating application software. APIs let digital products or services readily communicate with other products and services.
- **Algorithm:** A computer algorithm is a set of step-by-step instructions to perform a specific task.
- **Artificial intelligence (AI)**: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments (and operate with varying levels of autonomy). (OECD, 2020[24]) The goal of AI is to enable computers to automate some aspects of analysis—potentially saving human labour for more subtle tasks and gaining insights humans might not reach. There are several component technologies within AI all with numerous applications. There is no consensus as to what constitutes "thinking" and "intelligence" or what is "fully autonomous," and there are several categories of AI, but in general, to varying degrees, AI systems build "smart machines" that combine intentionality, intelligence, and adaptability. At present, machine learning is the most familiar and developed form of AI.
- **Big data:** The Financial Stability Board defines big data as "the massive volume of data that is generated by the increasing use of digital tools and information systems," such as financial transaction data, social media data, and machine data (e.g., Internet of Things, computer and mobile phone data. (FSB, 2017[25])
- **Black Box**: Black box refers to AI/machine learning and other technologies that are opaque, non-intuitive and do not provide adequate information regarding their decision-making and predictions/results –i.e., black box technology lacks explainability.
- **Benchmarking**: Benchmarking is an approach to determining the actual and relative capabilities of a technology-based process, product or service and identifying performance gaps by testing it against the best performance being achieved for the function, task, or goal—whether within the particular entity or organisation, industry-wide, or achieved by a different industry—using hard performance data measured by specified benchmarking criteria. Benchmarking may be used to measure [compare] the performance of new

technology vs legacy systems, or one new technology against alternative new technologies.

- **Collaborative Analytics:** For collaborative analytics, data is not moved to a central location in order to analyse them together with other data assets. Instead, the analytical tools come to the data, not the other way around. This makes it easier to keep the data secure and to ensure control over who accesses what data for what purposes.
- **Cybersecurity:** Cybersecurity, a broader term than data security, refers to the comprehensive process of protecting data and the systems for moving, storing, and authenticating that data.
- **Data pool/pooling**: Data pooling refers to a process where digital data from different sources are combined, resulting in a fuller and more useful data set for analysis (including by multiple parties). These pools are organised in a centralised manner.
- **Data security:** Data security refers to the process of protecting data from unauthorised access and data corruption throughout its lifecycle. It includes data encryption, hashing, tokenisation, and key management practices that protect data across all applications and platforms. Data security is narrower than cybersecurity.
- **Data standardisation**: Data standardisation is the process of converting data to a uniform format to enable users to process and analyse it. Data standardisation is essential to enable big data processing and advanced analytics, and the development and application of other innovative digital tools and methodologies. For example, financial data can vary within and across entities; data standardisation converts it into a common form that enables sophisticated large-scale analytics.
- **Digital Identity (ID) Systems/solutions:** Digital ID systems/solutions are identity systems or products and services that carry out the process of identifying/verifying a (natural or legal) person's identity, binding the proofed identity to a digital credential, and using the digital credential(s) and potentially other authentication factors to establish (confirm) that a person claiming the identity is the identity proofed person (i.e., is who the person claims to be).
- **Distributed Ledger Technology (DLT) (a.k.a. blockchain):** DLT refers to a type of technology protocol that enables simultaneous access, validation, and updating of an immutable ledger (digital record) distributed across multiple computers (and typically, across multiple entities or locations)—i.e., DLT creates a distributed digital database.
- **Deep Learning (DL):** DL is an advanced type of machine learning in which artificial neural networks (algorithms inspired by the human brain) with numerous (deep) layers learn from large amounts of data in highly autonomous ways. DL algorithms perform a task repeatedly, each time tweaking it a little to improve the outcome, enabling machines to solve complex problems without human intervention.
- **Digitalisation:** Digitalisation is the use of digital technologies and digitised data to change a business model, impact how work gets done, transform how

customers and companies interact, and provide new revenue and value-producing opportunities.

- **Digitisation:** Digitisation is the conversion of data, information, text, pictures, sound or other representations in analogue form into a digital form (i.e., binary code) that can be processed by computer.
- **Dynamic data:** Dynamic data refers to a continuous real-time digital stream of data points that are known to be in constant flux, so that the data set constantly changes over time, as distinct from static or persistent data that is mostly unaffected by time.
- **Explainability**: In the context of new technologies, explainability means that technology-based processes, solutions, or systems are capable of being explained (explicated), understood, and accounted for. Explainability provides adequate understanding of how solutions work and produce their results. Explainability is a basic condition for trust and responsible use. Explainable AI technology provides transparency into the data, variables and decision points used to achieve a result.
- **FinTech:** FinTech refers broadly to the use of new and emerging digital technologies in the financial sector for any of a wide variety of purposes. Initially, "FinTech" primarily referred to the application of technology-based innovations to provide new customer-facing financial products and services [e.g., mobile payment solutions, online marketplace lending, algorithmic savings and investment tools, virtual currency payments, capital raising (crowd funding) and deposit taking (remote check capture, mobile banking)]. FinTech now also encompasses the use of new and emerging technologies to provide automated mid- and back-office enterprise functions, such as the use of algorithms, big data, AI and machine learning, and link analytics for wholesale clearance, settlement, and other wholesale intermediation for e.g., securities, derivatives, wholesale finance, and payments, as well as regulatory compliance activities (see RegTech definition, below). Other applications remain to be developed
- **Fuzzy logic:** Fuzzy logic is a subset of AI that takes an open, imprecise spectrum of data (imprecise input) and processes multiple values in a way that produces output that includes a range of intermediate possibilities between YES and NO (e.g., certainly yes, possibly yes, cannot say, possibly no, certainly no). Fuzzy Logic systems produce definite output in response to incomplete, ambiguous, distorted, or inaccurate (fuzzy) input, simulating human decision making more closely than conventional yes/no logic. Fuzzy logic can be implemented in hardware, software, or a combination of both.
- **Internet of Things (IoT):** The global network of all Internet-enabled devices and machines that are connected to the Internet and can collect, send, share and act on data, using embedded sensors, processors and communication hardware, without human interaction. The IoT generates an enormous amount of real-time data that can be analysed and used to create desired actions or business outcomes (see big data).
- **Interoperability**: refers to the ability of different information technology systems and software applications to communicate, exchange data, and use

the information seamlessly in real-time, enabling all participants operate across all systems.

- **Machine Learning:** Machine learning is a type (subset) of AI that "trains" computer systems to learn from data, identify patterns and make decisions with minimal human intervention. Machine learning involves designing a sequence of actions to solve a problem automatically through experience and evolving pattern recognition algorithms with limited or no human intervention—i.e., it is a method of data analysis that automates analytical model building.
- **Machine Readable Regulation:** Machine readable regulation replaces rules written in natural legal language with computer code to enable the use of artificial intelligence for regulatory reporting purposes.
- **Natural language processing (NLP):** NLP is a branch of AI that enables computers to understand, interpret and manipulate human language. NLP allows humans to talk to machines.
- **Privacy Enhancing Technologies:** "Specialist cryptographical capabilities, which allow computations to take place on underlying data, without the data owner necessarily divulging that underlying data. The same technology can ensure that the data owner does not have visibility over the search query, with the query and the results remaining encrypted (or not disclosed) and only visible to the requester." (Maxwell, 2020[26]) This term therefore encompasses an array of technologies that use encryption and would be useful primarily in allowing the protection of privacy as data is used.
- **Real-time analytics:** Real-time analytics is a machine learning process in which a system processes and analyses data that is loaded instantaneously and almost immediately (in near- real time) generates meaningful output (e.g., information, predictions, or decisions).
- **Real-time data (RTD):** RTD is information that is delivered immediately after collection, ensuring the timeliness of the information provided. RTD enables real-time analytics and can be dynamic or static (e.g. a fresh input indicating a specific location at a specific time).
- **Regulatory Technology (RegTech):** RegTech is a sub-set of FinTech that uses new technologies to comply with regulatory requirements more efficiently and effectively than existing capabilities
- **Responsible Innovation:** Innovation is responsible when it is fit for purpose and complies with applicable regulatory requirements, including AML/CFT, consumer protection, cybersecurity, and privacy protections.
- **Smart machines:** Computer hardware and software systems that use AI algorithms. Smart machines are designed to make decisions, often using real-time data. Unlike passive machines that are capable only of mechanical or predetermined responses, smart machines use sensors, digital data, and remote inputs, combine information from these different sources, analyse this input instantly, and act on the insights derived from the data. Smart machines mimic human intelligence by using advanced computational process to reach conclusions based on their instant analysis.

- **Static data:** Static data refers to a fixed data set—data that remains the same after it is collected.
- **Supervised learning**: Supervised learning is a machine learning process that teaches algorithms predictive models by feeding the algorithm input data with known outcomes—i.e., supervised learning teaches algorithms by example. The input/output pair (labelled data) provides feedback for the algorithm, which uses the training data set to adjust the model to minimise error. For example, a training set may contain pictures of different kinds of animals with a label associated to each picture, allowing the algorithm to compare the predicted label with the correct one. Supervised learning uses a validation data set to measure the algorithm's progress in learning the model and a test data set to evaluate the model's performance on never-before-seen data to determine whether the model has learned its training data effectively and can generalise to new data.
- **Supervisory technology (SupTech):** SupTech is the use of innovative technology by supervisory authorities to support supervision and examination.
- **Unsupervised learning (a.k.a. unsupervised machine learning**): Unsupervised learning is a machine learning process that enables algorithms to analyse and cluster *unlabelled* datasets to discover hidden patterns, data groupings or anomalies or anomalies without human intervention. The algorithm parses available data and determines correlations and relationships without an answer key by drawing inferences and grouping like things based on unconstrained observation and intuition. As the amount of data the algorithm is exposed to grows, its modelling becomes more accurate and refined.

Annex B: Suggested Actions to Support the Use of Technology in AML/CFT

A responsible use of new technologies, including digital identity and cutting-edge transaction monitoring and analysis solutions (including collaborative analytics) can assist effective, risk-based implementation of the FATF Standards by the public and private sectors, as well as promote financial inclusion.

The following principles advance the San Jose Principle to *pursue positive and responsible innovation* endorsed by FATF in 2017. New technologies for AML/CFT must be developed and implemented in a way which reflects threats as well as opportunities, ensuring that their use is compatible with international standards of data protection and privacy, and cybersecurity.

1. Create an enabling environment by both government and the private sector for responsible innovation to enhance AML/CFT effectiveness:

i. Innovative solutions that facilitate the implementation of AML/CFT measures, including risk assessments, CDD and other requirements, and strengthen their supervision and examination.

ii. Good practices for updating internal legacy systems or replacing them with new technologies.

iii. Appropriate safeguards and features for new AML/CFT solutions, including: explainability and transparency of processes and outcomes; oversight by humans; respect for privacy and data protection; strong cybersecurity; and alignment with global, national, and technical standards and best practises.

2. Ensure Privacy and Data Protection when implementing new technologies:

i. Ensure there is a valid legal basis for the processing of personal data when deploying new technologies.

ii. Protect personal information in line with national and international legal frameworks.

iii. *Process data for an explicit, specified and legitimate purposes, consistent with national and international rules.*

iv. *Support the responsible development and adoption of innovative privacy-preserving technologies to enable robust AML/CFT information sharing and analysis, while preserving privacy.*

3. Promote AML/CFT innovation which supports financial inclusion by design

i. Mitigate the obstacles to financial inclusion through the development and implementation of innovative solutions

ii. Ensure responsible innovation consistent with the FATF objective to promote financial inclusion

4. Develop and communicate policies and regulatory approaches to innovation that are flexible, technology-neutral, outcomes-based and in line with the risk-based approach

i. *Consider the impact of new technologies holistically, in the context of the structural and organisational changes that accompany them, their possible unintended consequences, and their overall impact on AML/CFT effectiveness, and financial inclusion.*
ii. *Issue and/or update clear policy statements, guidance, use cases, best practises or regulations, as necessary to inform and encourage the responsible use of new technologies for AML/CFT*
iii. *Consult with counterparts and regulated entities to inform relevant policy and decision-making processes.*

5. Exercise informed oversight

i. *Build expertise in new technologies, to enable informed regulation and supervision of their use, including for specific AML/CFT compliance purposes.*
ii. *Identify explicit, well-defined uses of new technologies for AML/CFT supervision and examination*
iii. *Understand the risks and benefits associated with new technologies, and appropriate risk-mitigation measures that preserve their benefits.*
iv. *Use technology to enhance AML/CFT supervision*

6. Promote and Facilitate Cooperation

i. *Co-operate and co-ordinate with all relevant authorities to facilitate a comprehensive, coordinated approach to understanding and addressing risks and benefits in the use of new technologies for AML/CFT, including data protection and privacy authorities.*
ii. *Consider developing collaborative environments to facilitate cross-government and/or public private research and development of new technologies and innovative solutions.*
iii. *Participate in international efforts to develop global principles governing the use of new technologies for AML/CFT to help ensure their alignment with human rights, the improvement of the implementation of global AML/CFT, cybersecurity, data privacy and protection measures, as well as relevant technical standards and trust frameworks.*

Annex C: Case Studies

Brazil

The Central Bank of Brazil's Integrated System for Supervision Support (SisCom, APS-Siscom from 2018 on) is a 2014 web-based system, supported by a strong methodology, which allows interaction with supervised entities (SE) in a secure environment and facilitates the supervisory work in the following aspects:

- An easy and secure way for requiring and receiving from SEs policies, manuals, managerial reports, audit reports, files regarding KYC of specific clients and specific transactions, as well as SE's replies written into the system;
- Features for interaction during the inspection in order to clarify any issue and require complementary information or explanations;
- Standardizing inspection procedures, allowing various inspections to take place simultaneously;
- Inspection templates: BCB supervisors can create tailored requisition forms for a group of SEs, SEs sector or a SE in particular, which are stored in a portfolio for later use. A query feature allows supervision to know how many SEs any requisition was sent to;
- Producing reports: APS-Siscom provides automatically supervisory reports which can be readily assembled as a dossier for auditing purposes;
- At the end of the inspection, deficiencies and breaches are communicated through the System and SEs are required to present, also through APS-SisCom, a correction plan subject to supervisor approval;
- All the due dates are controlled and signaled by APS-SisCom, which provides an up-to-date tally of deficiencies and breaches' according to their completion status in a Business Intelligence report;
- Query features allows supervision to gather information on every inspection conducted on a specific SEs in order to track progress.

In 2018, Siscom was incorporated in the new BCB supervision platform SisAPS, which integrates several systems and databases. SisAPS were implemented for inspectors, supervisors and managers, providing a record panel of what the team is carrying out or has carried out in each inspection, as well as managerial information and monitoring reports.

APS-SisCom provided an enormous gain in productivity for the BCB's

supervisory teams, facilitating inspection procedures and allowing BCB to not perform time-consuming visits to SEs.

The data collected by APS-Siscom also feeds into a methodology, which allows BCB to segment and supervise banks and non-banking financial institutions (NBFI) by different risk categories. The quantitative and qualitative data are processed and analyzed by the supervisors to provide them with different perspectives:

- level of compliance with specific regulatory requirements;
- risk assessment, using a rating categorization.

As a result, this tool and methodology is enabling effective AML/FT supervision of hundreds of medium and small SEs spread all over Brazil's large territory.

HKMA: The role of the regulator in encouraging the use of network analytics

Working closely with banks, the Hong Kong Monetary Authority (HKMA) has over the past few years taken a number of steps to encourage the exploration and responsible adoption of AML/CFT Regtech applications, including through its Fintech Supervisory Sandbox and Chatroom and an AML/CFT Regtech Forum in November 2019. Amongst many applications, the HKMA has identified the development of network analytics applications as one of the HKMA's supervisory priorities, which support banks to add greater value to outcomes being achieved through Hong Kong's public private partnership - the Fraud and Money Laundering Intelligence Taskforce. Throughout 2020, the HKMA has been engaging banks to better understand the factors and dependencies affecting network analytics applications, which helps the HKMA as the supervisor to prepare responses, particularly to those banks who are asking *'how do we prepare to start using network analytics?'*

The HKMA has recently shared a case study of a bank which has been studying potential applications of network analytics for several years. (HKMA, 2021[27]) The bank's adoption of analytics is tracked since 2013 by detailing how it was used to enhance the bank's ability to identify a network demonstrating high ML/TF risk. The HKMA has illustrated how this bank overcomes certain challenges and some of the results that have been obtained.

To continue supporting the roadmap to accelerate adoption in the banking sector, the HKMA has communicated Regtech as a key focus in its 2021 AML/CFT supervisory programme and detailed how it will use some of the practices outlined in its recent publication to build industry acceptance of key technologies and create the conditions for all banks to explore and use Regtech in AML/CFT work, including network analytics.

Monetary Authority of Singapore

Problem statement

MAS supervises financial institutions (FIs) for their money laundering and terrorism financing (ML/TF) risk management. To enhance our supervisory effectiveness, we conduct risk surveillance to detect systemic risks and to target higher risk areas and FIs for closer supervisory scrutiny. Our FIs file Suspicious Transaction Reports (STRs) on potentially illicit flows of funds and financial crime concerns, and these provide useful information for our risk surveillance purposes. Complex typologies often involve multiple accounts at multiple FIs and this may manifest in multiple STRs filed over a period of time. Therefore, we have developed an STR network analytics tool to help us join the dots across FIs, and across time.

Insights and outcomes

The use of the STR network analytics tool has helped MAS identify concerning clusters of individuals/entities that exhibited suspicious behaviours, as well as the FIs involved for our supervisory analyses and scrutiny. This helped sharpen our ability to prioritise and target risks in our AML supervision. The insights and emerging risks uncovered from the network analyses are also shared with the financial sector through various platforms, including our AML/CFT Industry Partnership (ACIP), industry workshops, or via advisory notes and supervisory guidance to all FIs. These data driven engagements have raised industry risk awareness, and in turn have prompted FIs to expedite their adoption of innovative data analytics approaches to combat financial crime.

Other than furthering our supervisory objectives, the insights gained from the STR network analytics tool also aided in our national effort to combat financial crime. In Singapore, there is an interagency committee that brings together relevant law enforcement and supervisory agencies to investigate and develop risk mitigation plans for priority ML/TF cases. Several concerning networks detected through our STR network analytics have been escalated to that interagency committee for deliberation and coordinated action across agencies.

The data inputs for our network analyses in the initial phase comprise mainly information from the structured data fields in the STRs. We are in the process of enhancing the dataset to increase the impact of our network analytics tool. Firstly, we are developing natural language processing (NLP) models to extract information from the unstructured, textual data within STRs, e.g. narratives explaining the unusual nature of the customer's transactions and relationships between counterparties for ingestion into our network analyses. Secondly, our analytics tool has also started to ingest more transaction data and companies' profile information. These enhancements will strengthen our ability to identify hidden connections, and to detect and prioritise systemic risk concerns for supervisory and inter-agency follow-up.

Malaysia

Sandbox Framework to Facilitate Effective Implementation of e-KYC Regulatory Requirements

The Financial Technology Regulatory Sandbox (Sandbox) established by Bank Negara Malaysia (BNM) plays a pivotal role in promoting innovation in the financial industry, since 2016. It serves as an effective platform for BNM to monitor potential impact of innovation to the industry prior to setting out formal regulatory requirements on the industry.

The benefits of Sandbox is manifest, amongst others, in the growth of innovative business model in the Money Service Business (MSB). Prior to 2017, Malaysian MSB players were not permitted to undertake any transaction without face-to-face contact with new customers, unless business relationship with the customer had been first established and customer due diligence measures had been conducted. Through the Sandbox, two digital MSB players were able to test out their innovative business model including the use non face-to-face customer on-boarding process via the e-KYC solution, within an environment where risks associated with the new innovation can be adequately mitigated.

Taking into consideration the lessons learnt from the Sandbox, a regulatory requirement on non face-to-face on-boarding verification for MSB sector was introduced by BNM in end-2017. This has enabled a larger pool of qualified MSB players to implement e-KYC verifications, with proper safeguards such as establishing independent contact with customer and setting of transaction limits. To date, seven remittance companies have been approved to conduct e-KYC for on-boarding of new customers. BNM also took a gradual approach to roll-out the regulatory requirement in support of innovative solution in line with industry readiness. For instance, the e-KYC verifications was first introduced to the remittance segment and was extended to the money-changing segment in 2019.

Further to this, in accelerating and streamlining practices of industry players, BNM issued a revised AML/CFT policy document and e-KYC policy document applicable to all financial institutions in 2020 setting out regulatory expectations on the adoption of e-KYC technology among the institutions.

Annex D: Additional RegTech case studies for the uses of new technologies for AML/CFT

Case Study: Machine Learning-powered Smart Alert Management for AML Transaction Monitoring & Name Screening

A financial institution teamed up with Singapore-based regulatory technology (RegTech) company in its anti-money laundering (AML) fight. The collaboration has resulted in a holistic machine learning solution that would enable the financial institutions to draw out faster and more precise information to prevent and detect suspicious money laundering activities. The solution addressed two main processes within the Bank's AML framework -- transaction monitoring and name screening – effectively creating workflows for prioritising alerts based on their risk levels to help the compliance team focus on those alerts that matter the most.

The solution combines supervised and unsupervised machine learning techniques that seek to detect suspicious activities and identify high-risk clients quicker and more accurately. It offers an intelligent way to triage transaction monitoring and name screening alerts by segregating them into three risk buckets – L1, L2 and L3 – where L3 being the highest-risk bucket.

The transaction monitoring module is able to prioritise known alerts based on their risk scores and detect new, unknown suspicious patterns. The name screening module has three core components – enhanced name matching through a wider range of complex name permutations, reduction of undetermined hits through inference features and accurate alert detection through primary and secondary information. These capabilities help accurately distinguish between false hits and true hits.

This tool features a self-learning mechanism for automatic, continuous learning and a patent-pending explainable AI framework for a thorough understanding and to conduct a quality investigation. The framework explains the rationale behind each alert prediction by the machine learning model in a manner comprehensible to business users.

When it spots a pattern of suspicious activity, the AMLS also creates a smart rule and adds it to the AML typology library, thus enabling the machine learning models to detect similar patterns for future alerts. This means that over time, the solution will continue to filter the number of false positives and enable more accurate tracking. As such, the Bank's employees would be able to use the time saved to conduct more in-depth investigations on suspicious cases or to focus on other cases quickly and efficiently.

Case Study: Risk Management Solution

A multinational financial institution is using big data and automated Contextual Monitoring to detect and disrupt financial crime in international trade.

Contextual Monitoring is the ability to join and connect together data from different systems and sources to create context and meaning to identify significant connections and improve accuracy. It employs advanced algorithms which allow more sophisticated scoring and analytical approaches.

Using this technology, customer activities can be continuously assessed and scored for risk. This level of contextual monitoring improves accuracy, and decision-making, while providing insight into data relationships never before possible through an analytical and intelligence based AML solutions.

Its main benefits are: improved customer focus through fewer and higher quality alerts, identification of high risk activity tied to money laundering, the ability to provide full context of customer historical transactions and risk profile, the ability to provide transactional and non-transactional analysis of events.

Case Study: Robotic Process Automation solutions

A financial institution is developing initiatives based on Robotic Process Automation (RPA) solutions that allow to improve processes' efficiency like investigations of suspicious transactions, the screening of names to identify PEPs, the KYC on-boarding and recertification. Some natural language solutions (translation) are also used.

Current Machine learning solutions in place specifically on AML detection field include rule based models combined with data analytics, rule based models combined with alert scoring methodology, enriched rule based models (with external data such as company registry data) (not related to RPA in this case).

Case Study: Digital ID solution

A membership body is delivering solutions to champion innovation. This project aims to develop a scheme that will enable a single Digital ID that meets all relevant regulatory requirements (KYC and AML) and is positioned to consumers, as the prime means for securely identifying themselves to UK Financial Services.

The organisation is working closely with the Government to develop a National Trust Framework so the scheme will allow the consumer to use their Digital Identity across multiple sectors through having interoperable standards and technologies, it will rely on a variety of access points and proliferation of devices requiring ID authentication to synthesise the services and experience. It will also depend on increased usage of biometrics/video KYC, machine learning, NLP and blockchain/distributed ledger technology.

This Digital ID scheme will allow consumers to re-use their verified identity and associated KYC attributes to open and access online financial services.

Case Study: Risk and compliance firm addresses issues of data quality and consistency

One of the key pieces for proper risk scoring transactional data is the identification of all parties and geographies mentioned. This can prove to be challenging given the various transactional formats, combined with human error and/or attempts by bad actors to obfuscate their identity. To overcome these challenges the RegTech team employs various techniques to extract and normalize data.

This risk and compliance regulated entities offers a technology based data handling service to facilitate compliance with AML/CFT obligations. At the start of any project and prior to data acquisition, a series of conversations will occur with the stakeholders, SME's, and the necessary technical teams, to identify key data elements (KDEs). Once the data is in hand, the team creates a copy of the original (Golden

Source) to preserve integrity and auditability. Next, it performs high level analytics to better understand the data integrity and identify gaps.

String normalization is also an important part of this process. Removal of special characters, extra white space, and common corporate terms (LLC, OOO, Limited) are just a few of the steps taken to allow for better grouping, classification, and identification.

Entity extraction is an essential component of any risk model and is complicated by "dirty" or incomplete data. While there is a focus on the KDEs identified in the data acquisition process, reliance solely on this can miss "hidden" entities.

One technique that is commonly used is Natural Language Processing or NLP to identify parts of speech. NLP provides the ability to scan the entire dataset for proper nouns which could indicate an individual or company. While NLP is helpful, results still require additional analysis and cleansing as transactional data rarely follow typical grammar. Therefore, these scans are supplemented by internal intelligence of the tokenized string

Using the normalized entities extracted from early, the team creates a unique list while still maintaining lineage back to its original source.

References

BGIN (n.d.), *Blockchain Governance Initiative Network (BGIN), About*, https://bgin-global.org/about/. [23]

BIS (2020), *FSI Insights on policy implementation*, http://www.bis.org/fsi/publ/insights29.pdf. [31]

BIS (2019), *Suptech applications for AML, FSI Insights N.8*, https://www.bis.org/fsi/publ/insights18.pdf. [34]

Broeders D. and Prenio J. (2018), *Innovative technology in financial supervision (SupTech) – the experience of early users*, https://www.bis.org/fsi/publ/insights9.pdf. [36]

Chase, I. (2020), *Doing What is Right: Financial Inclusion Needs Better Incentives*, RUSI, https://rusi.org/commentary/doing-what-right-financial-inclusion-needs-better-incentives. [12]

CoE (2011), *Resolutions 1797 (2011), The need for a global consideration of the human rights implications of biometrics*, https://pace.coe.int/pdf/8b5e492cf90ea25e1c1f2f459c42bc9570713dd10154b339883da5da4c309a89/resolution%201797.pdf. [17]

Coelho et al. (2019), *Suptech applications for anti-money laundering*, https://www.bis.org/fsi/publ/insights18.htm. [4]

EBA (2021), *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks-across-eu. [11]

EBA (2020), *European Banking Authority, Big Data and Advanced Analytics*, http://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf. [30]

EC (2019), *30 Recommendations on Regulation, Innovation and Finance*, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf. [19]

FATF (2021), *Second 12-month Review Virtual Assets and VASPs*. [38]

FATF (2020), *Guidance on Digital ID*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html. [8]

FATF (2020), *Priorities for the Financial Action Task Force Under the German Presidency*, http://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf. [3]

FATF (2020), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/data-pooling-collaborative-analytics-data-protection.html. [37]

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. [1]

FATF (2014), *FATF clarifies risk-based approach: case-by-case, not wholesale de-risking*, http://www.fatf-gafi.org/documents/documents/rba-and-de-risking.html. [5]

FATF (n.d.), *FATF Guidance - The Risk-Based Approach*, http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate). [6]

FSB (2020), *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*, p. 32, http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory-technology-by-authorities-and-regulated-institutions-market-developments-and-financial-stability-implications/. [28]

FSB (2019), *Decentralised financial technologies – Report on financial stability, regulatory and governance implications*, http://www.fsb.org/wp-content/uploads/P060619.pdf. [21]

FSB (2017), *Artificial intelligence and machine learning in financial services*, https://www.fsb.org/wp-content/uploads/P011117.pdf. [25]

G20 (2019), *G20 Osaka Leaders' Declaration*, http://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html. [22]

G20 (2016), *High Level Principles for Digital Financial Inclusion*, https://www.gpfi.org/sites/gpfi/files/documents/G20-HLP-Summary_0.pdf. [9]

HKMA (2021), *AML/CFT Regtech: Case Studies and Insights*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf. [27]

HKMA (2020), *AML/CFT Supervision in the Age of Digital Innovation*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200929e1a1.pdf. [35]

Hong Kong Monetary Authority/Deloitte (2021), *AML/CFT Regtech:Case Studies and Insights*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf. [15]

Kazzaz, Z. (2020), *Emergency Disbursements during COVID-19: Regulatory Tools for Rapid Account Opening and Oversight*, p. 13, http://www.findevgateway.org/sites/default/files/publications/submissions/72016/Emergency%20. [13]

MAS (2018), *Industry Perspectives – Adopting Data Analytics Methods for AML/CFT*, http://www.mas.gov.sg/regulation/external-publications/industry-perspectives-adopting-data-analytics-methods-for-amlcft. [18]

Maxwell, N. (2020), *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime*, http://www.future- [26]

fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf.

OECD (2020), *AI Principles*, https://www.oecd.ai/ai-principles. [24]

Richard Grint et al (2017), *New Technologies And Anti-Money Laundering Compliance*, FCA, http://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf. [14]

SAS (n.d.), *Five AI technologies that you need to know*, https://www.sas.com/en_us/insights/articles/analytics/five-ai-technologies.html. [29]

UN (2019), *United Nations Security Council (UNSC) Resolution 2462 (28 March 2019), UN Doc S/RES/2462, para.20*, https://undocs.org/en/S/RES/2462(2019). [2]

UN (2018), *Compendium Of Recommended Practices For The Responsible Use & Sharing Of Biometrics In Counter Terrorism*, https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf. [10]

Vyjayanti T Desai et al. (2018), "The global identification challenge: Who are the 1 billion people without proof of identity?", https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity. [7]

Walshe, P. (2020), *Digital Identities*, https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc-en/1680a0c051. [32]

WEF (2020), *Forging New Pathways: the next evolution of innovation in financial services*, http://www.weforum.org/reports/forging-new-pathways-the-next-evolution-of-innovation-in-financial-services. [33]

World Bank (2021), *Principles On Identification For Sustainable Development: Toward The Digital Age*, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/470971616532207747/principles-on-identification-for-sustainable-dev. [16]

Yuta Takanashi et. al (2020), *Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem, Part 2 of 2*, https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance2/release/1. [20]

OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT

New technologies can improve the speed, quality and efficiency of measures to combat money laundering and terrorist financing. They can help financial institutions and supervisors assess these risks in a more accurate, timely and comprehensive manner. When implemented using a responsible and risk-based approach, new technologies can also improve financial inclusion.

This report identifies emerging and existing technology-based solutions. It highlights the necessary conditions, policies and practices that need to be in place to successfully use these technologies and improve the efficiency and effectiveness of AML/CFT. It also examines the obstacles that could stand in the way of successful implementation of new technology.

www.fatf-gafi.org | JULY 2021