NEW TECH, PERPETUAL CHALLENGES

How Emerging Technologies for Financial Compliance are Impacting the Nonprofit Sector

A report prepared by:
ECNL – European Center for Not-for-Profit Law
Rita R. Soares, LL.M.
Dr. Tasniem Anwar
Dr. Mara Wesseling

Program

This report was prepared as part of the program on Security and Counter-Terrorism of the European Center for Not-for-Profit Law Stitching (ECNL). It represents the preliminary findings and recommendations of ECNL's working group researching how emerging technologies for AML/CFT are impacting the nonprofit sector.

Acknowledgements

The authors are grateful to the National Endowment for Democracy for making this report possible and to the institutions, experts, and practitioners who kindly shared their insights with ECNL.

All trademarks and graphics included in this report are acknowledged as the property of the respective owners.

Disclaimers

The information contained in this report is true and accurate to the best of the authors' and ECNL's knowledge and ability. The authors made every effort to ensure the accuracy of this publication but cannot be held liable for any loss or damage (direct or indirect), however caused, arising in any way from any information or recommendations contained in this report.

June 2022

Copyright © 2022 by ECNL. All rights reserved.

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

Table of Contents

List of Acronyms and Abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
DLT	Distributed Ledger Technologies
DPIA	Data Protection Impact Assessment
ECNL	European Center for Not-for-Profit Law Stitching
FATF	Financial Action Task Force
FI	Financial Institution
FinTech	Financial Technology
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
IMF	International Monetary Fund
Inc.	Including
KYC	Know Your Customer
ML	Machine Learning
NLP	Natural Language Processing
NPO	Nonprofit Organisation
OCR	Optical Character Recognition
PEP	Politically Exposed Person
RegTech	Regulatory Technology
Snr	Senior
SupTech	Supervisory Technology
Tech	Technology
US	United States of America

Executive Summary

Over the past decade, financial and regulatory technology has grown exponentially, with new technologies promising to make compliance with AML/CFT measures faster, cheaper, and more effective. Compliance solutions powered by technologies such as big data analytics, artificial intelligence, machine learning, Blockchain, and distributed ledger technologies claim to reduce false positives and have the computational power to find increasingly sophisticated and complex financial crime patterns. These technologies are expected to increase efficiency in tackling financial crime far beyond human compliance checks. Furthermore, these technologies are also believed to improve the financial inclusion of underserved communities, including the nonprofit sector.

Under the current international AML/CFT regulatory framework, NPOs - and humanitarian relief organisations in particular - have fallen victim to the financial industry's tendency to de-risk in order to avoid financial penalties arising from regulatory noncompliance. As a result, NPOs face severe difficulties opening banking accounts, delayed transactions and unexplained account closures. Experts and international organisations such as the FATF and the IMF have argued that emerging tech solutions for AML/CFT compliance may reduce the obstacles faced by NPOs.

This report aims to fill the knowledge gap regarding the real-world impact of these emerging technologies on the NPO sector's access to financial services in an effort to determine what impact these tech solutions are having on civic space. Through interviews with financial institutions, FinTech companies, supervisors, and other experts, ECNL explored how responsibly these technologies are deployed in the financial sector from the perspective of NPO clients, often an afterthought for financial institutions.

In this study, our guiding principle is that public confidence in the technology used in the financial sector is critical to a well-functioning society. A lack of confidence in these technologies could result in a loss of confidence in the financial system as a whole. Trust and confidence should be sought not only from those engaged in designing or deploying technology but also from those expected to use and be affected by it. As such, both experts and non-experts should have or be able to find basic but reliable information regarding the abilities, risks and limitations of a given application in order to maintain a healthy level of informed trust in the system where those applications are deployed.

With that principle in mind, we first outline the kinds of emerging technologies used for compliance purposes, reviewing their high-level fundamentals and possible applications along the AML/CFT compliance chain. These technologies include supervised and unsupervised ML, NLP, OCR, APIs, fuzzy logic, phonetics, computational linguistics, cryptography, supervised algorithms such as decision

trees, random forests and logistic regressions, and clustering techniques like K-means algorithms and other big data analytics techniques.

Then, we focus on the de-facto conditions of design, development, deployment and operation of these compliance solutions, grouping the main findings under six key themes commonly linked to responsible technology development.

1. **Effectiveness & Reliability.** The most commonly cited benefits of emerging technologies for compliance were time savings, cost reductions, revenue generation and commercial growth. Private sector interviewees described the technology as more targeted and efficient, resulting in fewer false positives than manual compliance checks. Several FinTechs businesses framed their tools as amplifiers of human abilities, with a superior ability to assess probabilities and deal with complexity. Some claimed that extracting insights from unused data could also reduce de-risking and improve financial exclusion. However, most claims about the benefits harnessed by technology were hard to verify due to a lack of adequate metrics to measure the effectiveness and reliability of tech-powered tools. Furthermore, concerns over the state of advancement of these technologies were expressed. Non-private sector interviewees criticised the bluntness of some of these tools and showed scepticism regarding the precision of tech-enabled compliance checks. They commented that customer profiles often lack essential information and that data quality and data sharing remain significant issues. Privacy-enhancing technologies and public-private partnerships were discussed as potential - albeit not yet viable - solutions for the data quality issues.

2. **Fairness & Discrimination.** Compliance teams seem to prioritise accuracy and efficiency above outcomes such as fairness and financial inclusion. When asked about the risks associated with their technology, developers and operators focus heavily on risks related to the functioning of their systems (how they are built, how predictably they operate) but not so much on the systems' broader structural and societal impact. Businesses developing or using FinTech made scant disclosures about errors and did not always appear to have considered unintended consequences or reflected on the wider socioeconomic impact of their technology. We observed a difference between larger and more mature FinTech companies and financial institutions - which indicated reviewing fairness and bias before production - and start-ups and scale-ups - which seem to defer such non-mission-critical concerns to later in their journey or shift those priorities to end-users and customers. Stated commitments to promote fairness or avoid discriminatory effects were rarely accompanied by concrete measures to foster those values. Overall, our interviews did not show that businesses quantified discriminatory effects toward the NPO sector or installed safeguards against such risks. While emerging technologies for compliance are presented as more precise and therefore less discriminatory and more inclusive, it is not clear that they increase financial inclusion for NPOs.

3. **Security & Data Privacy.** Due to strict legal requirements such as the GDPR, cybersecurity and privacy concerns seem to be taken rather seriously by the private sector regardless of the

business' size or maturity. Even start-ups stated that data privacy is a priority. However, not much seems to be delivered to data subjects beyond the review of set terms and conditions and privacy policies designed to safeguard institutional interests. The observed practices are unlikely to afford financial services consumers genuine ownership and agency over their data and the inferences that can be extracted from it.

4. **Transparency & Explainability.** Much of what happens in financial institutions is intentionally not visible to the customers. Businesses seem to focus predominantly on ensuring automated decisions are explainable to operators, regulators and supervisors. Not much heed is paid to explaining the rationale behind decisions to the individuals ultimately affected by those decisions. A need for secrecy is frequently depicted as a necessary precaution against strategic classification and other risks, foreclosing any possibility of analysing and improving potentially flawed models. Without a baseline level of transparency toward a wide range of stakeholders (including non-experts and the general public, at times), there is no way to trust or verify that a given decision that has been aided or mediated by emerging technology can be explained or, if necessary, corrected. There is no basis to confirm that these applications adhere to normative or legal standards and produce fair results. There are no means to ensure that those engaged in the design, development, deployment, operation and validation of the effectiveness of these applications can be held accountable for negative outcomes.

5. **Human Oversight & Technical Competence.** The overwhelming response of our interviewees was that human oversight over the technology existed at all critical levels of the process, with human control over the final decisions. However, neither developers nor deployers of compliance technology painted a thorough picture of the conditions surrounding human control over algorithmically generated decisions. Furthermore, technology developers and procurers do not seem to set minimum technological literacy and competence standards or guidance for the technology operators. Some observations also suggest that the compliance analysts tasked with critical human oversight are often young graduates who received very theoretical knowledge, have not yet had their knowledge tested by real-world conditions, and are unlikely to expend extra time or effort gathering additional sources to judge the accuracy of algorithmic-made decisions. Overall, the data we gathered is indicative of human involvement but not necessarily of human control.

6. **Accountability & Contestability.** Our findings were inconclusive regarding who is responsible for the different stages of the technology pipeline and who is accountable for negative outcomes. In most cases, there is no concrete framework laying out who is responsible for what action, who has recourse to which corrective actions and what information will be disclosed to enable problem-solving procedures. There do not seem to be clear avenues for allocating responsibility between the agents involved in creating and operating a system. Our research also did not uncover any concrete procedures for contesting these decisions. Even when a technologically-enabled decision substantially impacts a person or group, the channels for challenging it are often not readily apparent or feasible.

Afterwards, we explore what our findings mean for the NPO sector, particularly concerning de-risking and financial inclusion. We found an inconsistent approach to NPOs across the financial sector. NPOs are often globally treated as high-risk customers due to generally misguided understandings of AML/CFT requirements. The possibility that this flawed approach will permeate the design and development of new technologies is especially concerning given the difficulties in challenging some of these decisions and the lack of in-depth knowledge about NPOs. Most FinTech businesses do not have actionable insights about NPOs. Many lack basic information about the needs and operation of NPOs and how their products impact NPOs and do not include representatives from the NPO sector in the teams responsible for designing and developing their technology. The evident lack of NPO-specific knowledge or participation suggests that tech solutions are not properly calibrated for NPOs (whose profile and behaviour differ from ordinary banking clients). Potential negative impacts or biases against NPOs will likely remain unnoticed and go unnoticed uncorrected. As they represent such a small group outside the set target demographic for most businesses, NPOs are unlikely to become a specific customer segment with a bespoke set of rules and procedures addressing their systemic issues. Even if emerging technologies could provide such solutions, incentives do not seem aligned for businesses to allocate their resources to designing technology with the NPO sector in mind.

Finally, we reflect on the main challenges and opportunities for improvement. We propose a number of recommendations throughout the report to improve aspects connected to the six key themes (Tables 1-6) and the technology's impact on NPOs (Table 7), as well as broader recommendations for the main groups of stakeholders in a position to move the ecosystem forward (Table 8).

While this report sheds an initial light on these matters, it also reveals and suffers from a general lack of interest of financial institutions and FinTech firms alike in engaging with external stakeholders on these issues. Further research is needed to examine how larger financial institutions make use of these technologies and how NPOs and their needs can be better integrated into the design, development and deployment of these technologies.

Comprehensive coverage of all the issues within our scope is not feasible in a single report. Therefore, we will expand this initial mapping exercise with reflections and experiences of NPOs and banking regulators and explore recent efforts by multilateral institutions such as the United Nations to use similar technologies for security and counter-terrorism purposes.

Introduction

The growth of financial and regulatory technology

In July 2021, the Financial Action Task Force (FATF), which establishes the international standards for anti-money laundering (AML) and combating the financing of terrorism (CFT), published a report on the potential of emerging technologies to make AML/CFT measures "faster, cheaper and more effective".[1] The report speaks to a broader development in the financial sector to deploy big data analytics, machine learning, and Blockchain technologies to conduct client due diligence and transaction monitoring.[2]

Financial institutions are under legal obligations to monitor their clients' transactions for suspicious activities and actively manage financial crime risk by investigating their clients. In an effort to reduce the cost and time spent on these financial compliance tasks, financial institutions have started to leverage new types of financial technology (FinTech) specifically focused on compliance, such as RegTech and SupTech.[3] The adoption of these technologies has grown exponentially in recent years.[4]

In a survey of people who work in compliance, nearly 60% of respondents stated RegTech had enhanced their ability to manage AML/CFT, know-your-customer (KYC), and sanctions compliance processes.[5] Between 2018 and 2023, the regulatory technology industry is expected to grow between 23% and 25% per year. By 2026, the global market for regulatory technology is expected to be worth $33.1 billion.[6]

The main drivers for this growth are easily understood. Costs associated with AML compliance have surpassed $40 billion in the United States alone and $200 billion

1 FATF, "Opportunities and Challenges of New Technologies for AML/CFT", 2021, Paris: FATF, p. 4.

2 FATF, "Opportunities and Challenges".

3 A brief note on terminology: the term FinTech is commonly used to describe any technology that assists financial service companies in operating or delivering their products and services or that supports businesses or individuals in managing their financial affairs. Two specific uses of FinTech are RegTech - technology used by financially regulated businesses (such as baking) to navigate their compliance and regulatory requirements - and SupTech - technology used by supervisory agencies in charge of monitoring compliance with regulatory requirements. Given the focus of this report on emerging technologies used for compliance purposes, we use the word FinTech broadly to encompass both RegTech and SupTech.

4 FATF, Opportunities and Challenges, see also: El Bachir Boukherouaa and Ghiath Shabsigh, "Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance", 2021, IMF Departmental paper 2021/024.

5 Woodsome, Jim, and Vijaya Ramachandran, "Fixing AML: Can New Technology Help Address the De-risking Dilemma." Center for Global Development, 2018, Washington DC: Center for Global Development, p. 5. Dow Jones and SWIFT, "Global Anti–Money Laundering Survey Results 2017", 2017, New York: Dow Jones. p. 36.

6 Sentinels.ai, "5 Ways AI Can Boost The Regtech Onboarding Process", 19 January 2022. Available at https://www.sentinels.ai/resources/5-ways-ai-can-boost-the-regtech-onboarding-process. (Accessed 22 Apr 2022)

globally.[7] Although money laundering is a criminal industry with an estimated yearly revenue of $2.8 trillion, the sums recovered through anti-money laundering measures are barely 0.1 per cent of the total.[8] Financial industry actors increasingly turn to technology to search for ways to improve these dire statistics.

Financial industry actors worldwide claim to be applying techniques such as deep learning, neural networks, natural language generation and processing, robotic process automation, application programming interfaces, and more in the context of their AML/CFT efforts. Concrete and potentially familiar applications include facial recognition software for customer verification, algorithms to detect suspicious financial transaction patterns in large data sets, and the automation of reporting processes.

These tech-powered solutions are being widely applied due to their ability to learn and adapt to changing and increasingly sophisticated criminal activities and detect suspicious behaviour, making risk assessments and reporting duties under the AML/CTF regime easier and faster. Furthermore, these technologies promise to reduce the number of false positives in the generation of AML/CTF alerts, allowing compliance officers to focus on a smaller number of alerts.[9]

In addition to the highlighted efficiency gains, the FATF also states that these technological solutions can ultimately improve financial inclusion. These technologies "minimise weaknesses in inconsistencies related to human control measures, improve customer experience, generate cost savings, and facilitate transaction monitoring".[10] Such improvements can furthermore result in "more inclusive and safe financial systems that do not discriminate on the basis of means, social or regional context".[11]

Financial institutions could gain a better understanding of their risk in serving high-risk clients by improving customer due diligence through advanced verification technologies and strengthening business relationships through behavioural analytics. Similarly, other experts have concluded that new technologies lower the costs for compliance, resulting in financial institutions becoming more willing to conduct business in high-risk sectors or geographies.[12]

7 Lexisnexis Risk Solutions, "True Cost Of Financial Crime Compliance Study Global Report." Lexisnexis Risk Solutions, September 2021. Available at https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report. (Accessed 22 Apr 2022)

8 Lucinity.com, "Productivity And Profitability: Rethinking The Role Of AML Compliance", 2 February 2022, https://www.lucinity.com/blog/aml-competitive-advantage. (Accessed 22 Apr 2022)

9 FATF, "Opportunities and Challenges".

10 FATF, "Opportunities and Challenges", p. 16.

11 FATF, "Opportunities and Challenges", p. 18.

12 Woodsome and Ramachandran, "Fixing AML".

In summary, these technological developments are presented as promising solutions to increase AML and CFT efficiency and financial inclusion outcomes for underserved communities, including NPOs.

The challenges faced by NPOs

The NPO sector has suffered the impact of AML/CTF measures disproportionately, as recognised by the FATF itself in a recent report addressing four key areas of unintended consequences of the AML/CFT measures on NPOs: de-risking; financial exclusion; suppression of nonprofit organisations or the nonprofit sector as a whole; and threats to fundamental human rights.[13]

The FATF has previously defined de-risking as "the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage risk in line with the FATF's risk-based approach".[14] ECNL has investigated this phenomenon comprehensively in recent publications.[15]

De-risking is fueled by several factors, including rising compliance costs, falling risk tolerances, and strict and narrow interpretations of AML/CFT standards by national-level regulators.[16] Within this context, NPOs are typically considered a high(er) risk sector, despite scarce evidence to that effect.[17]

NPOs often operate in disaster zones, conflict areas and other high-risk geographies. Financial institutions' risk scoring and profiling mechanisms track whether organisations work on "risky" issues or in "risky" areas and countries, building a specific risk profile of NPOs. Moreover, each financial institution adopts its own risk-based approach, which might not be consistent or entirely coherent, leaving the NPO sector to scramble for guidance that is often missing or difficult to understand, especially for smaller sized organisations. Finally, the daily operations and practices of NPOs often consist of behaviour that financial institutions consider inherently more suspicious, such as cash deposits, odd amounts and international money transfers, among others.

13 FATF, "High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards", 27 October 2021. Available at https://fatfplatform.org/news/high-level-synopsis-of-the/ (Accessed 25 May 2022).

14 FATF, "FATF clarifies risk-based approach: case-by-case, not wholesale de-risking, 23 October 2014. Available at https://www.fatf-gafi.org/documents/documents/rba-and-de-risking.html (Accessed 25 May 2022).

15 També, Noémi, "Unintended consequences of AML/CTF regulation: the challenges of banking non-profit organizations: A review of onboarding and monitoring practices across financial institutions", (2021), European Centre for Not-for-profit Law.

16 També, "Unintended consequences".

17 For example, after 9/11, the US focused on investigating and disrupting the financial behaviour of several charity organisations, such as Al-Barakaat. Islamic NGOs and charities in particular were flagged as connected to terrorist activities, based on little concrete evidence. For an overview of this see: Ibrahim Warde,"The price of fear. Al-Qaeda and the truth behind the financial war on terror". (IB Tauris, 2007).

The combined effect of high compliance costs and the complexity of NPO work make financial institutions reluctant to serve NPO clients.[18]

The 2021 FATF Stocktake of the Unintended Consequences of the FATF Standards[19] notes that, despite ongoing efforts, de-risking and financial exclusion remain challenges for many sectors and run contrary to the risk-based approach promoted by the FATF. This scenario results in restricted access to financial resources and bank accounts, intrusive questioning and surveillance and even the termination of banking relationships.[20] These issues negatively impact a broad range of agendas, including civic freedoms and civic space, the implementation of the UN Sustainable Development Goals[21] and the financial inclusion agenda in general. They also negatively affect the countering/preventing violent extremism agenda, as smaller, community-based organisations impacted by financial exclusion are crucial in preventing radicalisation that might lead to violent extremism. Finally, by pushing money transactions underground, they create new terrorism-financing risks.[22]

The knowledge gap

The FATF, the IMF and several experts posit that emerging technological solutions for compliance might reduce the obstacles faced by NPOs.[23] However, we have limited knowledge of the real-world impact of these emerging technologies on the NPO sector.

While examining the potential benefits of technological solutions for compliance is important, it is crucial to map their risks and unintended consequences across the spectrum of financial services users, including underserved and marginalised communities. The FATF report[24] acknowledges this need and includes a list of "unintended consequences and potential for abuse" in its review. Nevertheless, this list remains rather abstract. It does not address how technologies are developed and tested by FinTech companies, how financial institutions procure, deploy and operate these technologies, or what safeguards are installed to mitigate unintended harmful consequences to specific clients who may be adversely affected by novel technological approaches.

18 Warde, "The price of fear", see also Human Security Collective and European Center for Non-For-Profit Law, "At the Intersection of Security and Regulation: Understanding the Drivers of 'De-Risking' and the Impact on Civil Society Organizations", 2018; FATF, "High-Level Synopsis" ; NYU Paris EU Public Interest Clinic, "Bank De-Risking of Non-Profit Clients.", 2021, https://www.readkong.com/page/bank-de-risking-of-non-profit-clients-a-business-and-7767260 (Accessed 25 May 2022).

19 FATF, "High-Level Synopsis".

20 També, "Unintended consequences".

21 Human Security Collective and European Center for Non-For-Profit Law, "At the Intersection of Security and Regulation".

22 Human Security Collective and European Center for Non-For-Profit Law, "At the Intersection of Security and Regulation"

23 FATF, "Opportunities and Challenges"; Boukherouaa and Shabsigh, "Powering the Digital Economy"; Woodsome and Ramachandran, "Fixing AML".

24 FATF, "Opportunities and Challenges".

We still know very little about whether these new FinTech solutions are maintaining or exacerbating trends to de-risk NPOs or whether they are widening or shrinking civic space and affecting fundamental human rights. More in-depth research into the effects of emerging technologies on the issues of de-risking and financial exclusion faced by NPOs is needed.

Purpose and structure of the report

This study's purpose is to contribute to a better understanding of the effects of the use of emerging technologies for AML/CFT on the nonprofit sector, a demographic which has traditionally been adversely impacted by the financial industry's trend to de-risk in order to avoid financial penalties arising from AML/CFT regulatory noncompliance.

Intending to determine whether the increased reliance on FinTech for compliance purposes is maintaining or exacerbating this trend to de-risk (or, alternatively, enabling a more inclusive access to financial services that could benefit traditionally underserved demographics such as NPOs), ECNL reached out to several financial institutions, FinTech companies, supervisors, and other experts who shared their insights on what these technologies entail, how they are developed and deployed in the financial industry, and the impact those elements have on NPOs.

This report summarises the main findings of this preliminary research exercise. It aims to provide a nuanced outlook on the potential of emerging technologies for AML/CFT focused on the needs of a sector often overlooked by the financial and tech industries. Moving beyond binary tech-optimistic or tech-pessimistic perspectives, this report strives to focus on the real-world consequences, dilemmas, and pitfalls stemming from the use of financial technologies in compliance efforts from the NPO stance.

We present our findings in a three-part structure that mirrors the three research sub-questions which form the core of our inquiry:

I.	***Emerging technologies used for AML/CFT purposes***	What kinds of emerging technologies are used for AML/CFT?
II.	***Standards for technology design, development, deployment and operation***	How are these technological solutions designed, developed, deployed and operated?
III.	***Impact on the NPO sector***	Is this technology maintaining, exacerbating or mitigating issues for NPOs?

Section I focuses on mapping and reviewing the high-level fundamentals of different technologies used for compliance purposes and their possible applications along the AML/CFT compliance chain.

Section II provides an overview of the observed de-facto conditions for the design, development, deployment and operation of compliance solutions powered by emerging technologies. Our findings are grouped under six key themes commonly linked to responsible technology development: (1) Effectiveness & Reliability, (2) Fairness & Discrimination, (3) Security & Data Privacy, (4) Transparency & Explainability, (5) Human Oversight & Technical Competence, (6) Accountability & Contestability.

Section III explores what the previous section's findings mean for the NPO sector, particularly in regard to de-risking and financial inclusion.

While this report sheds an initial light on these matters, it also reveals and suffers from the lack of interest of financial institutions and FinTech firms in engaging with external stakeholders on these issues. Further research is needed to examine how larger financial institutions make use of these technologies and how NPOs and their needs can be better integrated into the design, development and deployment of these technologies.

Methodology

Research design

To map out the use of emerging technologies in the AML/CFT setting and their impact on the NPO sector, we subdivided the research topic into the three primary inquiry areas:

1. **What kind of emerging technologies are used for AML/CFT?**
2. **How are these technological solutions designed, developed, deployed and operated?**
3. **Is this technology maintaining, exacerbating or mitigating issues for NPOs?**

Afterwards, we developed a questionnaire loosely based on Annex B of FATF's "Suggested Actions to Support the Use of Technology in AML/CFT"[25] to better understand how these suggested actions are interpreted and implemented in practice. The aim was to use the questionnaire as a guide for semi-structured interviews to take place alongside conference attendance and desk-based research.

Finally, we compiled a list of target experts from the FinTech and financial industry sectors to interview. We reached out to the relevant individuals and organisations through existing networks (LinkedIn), recommendations (or "snow-balling") and the general contact details of the relevant companies and organisations.

The success rates from the outreach into the banking and FinTech sectors were low,[26] suggesting their reluctance or unwillingness to engage with ECNL (or perhaps the NPO sector in general) on this topic. We also noted the sample size of the initially secured interviews was limited, in the case of financial institutions, and skewed towards smaller[27] sized firms, in the case of FinTech firms. These limitations are further examined in the concluding chapter of this report.

In an effort to mitigate potential bias arising from the nature of the sample group, we expanded the initial scope of research to include think tanks and consultancies, in order to leverage their sector-wide birds-eye view of the issues a stake and corroborate individual data points gathered from the limited number of banking and tech sector interviews.

25 FATF, "Opportunities and Challenges".

26 In aggregate, we contacted 15+ financial institutions (with a success rate of 20%), 40+ smaller-sized FinTech firms (with a success rate of 15%), 20+ mid-sized FinTech firms (with a success rate of 5%) and 10+ larger FinTech firms (with a success rate of 10%).

27 In the context of this study we defined the size of companies with 0-50 employees as small, companies with 51-250 employees as medium and companies with more than 250 employees as large.

Data collection

Data for this study was collected primarily through video-conference interviews, requests for comment via email correspondence, conference attendance and desk-based research conducted between November 1, 2021 and April 20, 2022.

More than 20 experts from financial institutions, FinTech firms, supervisors, think tanks, research centres, policy institutes, financial services consultancy firms and law enforcement were interviewed or otherwise provided their insights on the relevant research topics. A list of the main research participants can be found in Appendix A.

Interviews were semi-structured and loosely based on the research questionnaire. The average interview length ranged was 30-60 minutes. Although in a few cases the interviews were recorded and later transcribed, they were predominantly documented through note-taking on the part of the researchers. Where the interviews took place in a language other than English, the English translations are the researchers' own. Expert insights were often paraphrased due to time constraints and for readability purposes.

Separately, researchers attended virtual conferences where they engaged with some of the conference speakers and tested product demos. This paper incorporates contributions from some of the conference participants.

Finally, the researchers conducted a desk-based review of governmental and non-governmental policies and reports, media reports and grey literature cited throughout this report.

Data analysis

The qualitative data thus collected was reviewed by our team of four researchers to identify themes and emerging patterns. Regular meetings were held to discuss initial emerging trends. Subsequently, inductive coding was performed to analyse the interview transcripts, reports, and field notes. The following chapter presents the most relevant findings.

Findings & Analysis

I. Emerging technologies used for AML/CFT purposes

What are emerging technologies for AML/CFT?

The FATF describes technologies for AML/CFT as "innovative skills, methods, and processes that are used to achieve goals relating to the effective implementation of AMLC/FT requirements or innovative ways to use established technology-based

Onboarding Verification	Transaction Monitoring	Client Monitoring	Regulatory Monitoring and Reporting
Facial biometrics for selfies and risk-scoring Open-sourced liveliness and blurriness detectors for selfies Onboarding name screening with sanctions and PEP screening Benchmarking for correspondent banking networks Name variation software based on phonetics Multilingual database searching and mapping Digitised, unified and embedded regulatory knowledge platform	Speciality models for transaction monitoring and anomaly detection Dynamic financial crime detection systems Advisory services and technology solutions to respond to risk, prevent compliance breaches, remediate issues and monitor ongoing business activities Transaction screening	Holistic, automated and continuously updated customer risk scoring tools Digitised, unified and embedded regulatory knowledge platform Auto-indexing of facts, events and information from unstructured text for adverse media checks	Advisory services and technology solutions to respond to risk, prevent compliance breaches, remediate issues and monitor ongoing business activities Digitised, unified and embedded regulatory knowledge platform

processes to comply with AML/CFT obligations".[28] As such, we cast a wide net in the hope of hearing from a diverse range of developers and operators engaged in making wor using such technology.

We had the opportunity to interview or otherwise hear live insights from FinTech companies and financial institutions whose business involves several technological solutions deployed across key AML/CFT processes.

In order to provide these compliance solutions, the research participants rely on technology such as supervised and unsupervised ML, NLP, OCR, APIs, fuzzy logic, phonetics, computational linguistics, cryptography, supervised algorithms such as decision trees, random forests and logistic regressions, clustering techniques like K-means algorithms and other big data analytics techniques. While a full-length description of each of these techniques would not be feasible in this report, a good primer on three main categories (Big Data applications and analytics, AI and ML, and Blockchain and DLT) can be found in a comprehensive report published by the Center for Global Development on AML.[29]

How does the use of these technologies change the compliance landscape?

Although a detailed analysis of the ways in which emerging technologies can alter the AML/CFT workflow is also not practical here, we include below a brief graphic overview of what the compliance chain could look like without and with technology. This information is meant to be illustrative rather than exhaustive, contextualising the discussion around benefits, risks and challenges presented by this technology in the following chapters of this report.

The FATF's main thesis is that better ways to gather and interpret data, as well as share it with relevant stakeholders, might benefit the compliance process in general and promote a more dynamic risk-based approach.[30]

Solutions based on AI and ML applied to big data can improve the ongoing monitoring and reporting of suspicious transactions. These technologies can monitor, process, and analyse suspicious transactions and other criminal activities in real-time, separating them from routine activity and decreasing the need for initial, front-line human assessment. AI and machine learning technologies and solutions can also offer more accurate and comprehensive evaluations of continuing client due diligence and risk, which can be updated in real-time to account for new and emerging risks.[31]

28 FATF, "Opportunities and Challenges".

29 Woodsome and Ramachandran, "Fixing AML".

30 FATF, "Opportunities and Challenges", p. 14.

31 FATF, "Opportunities and Challenges", p. 7.

The AML Process

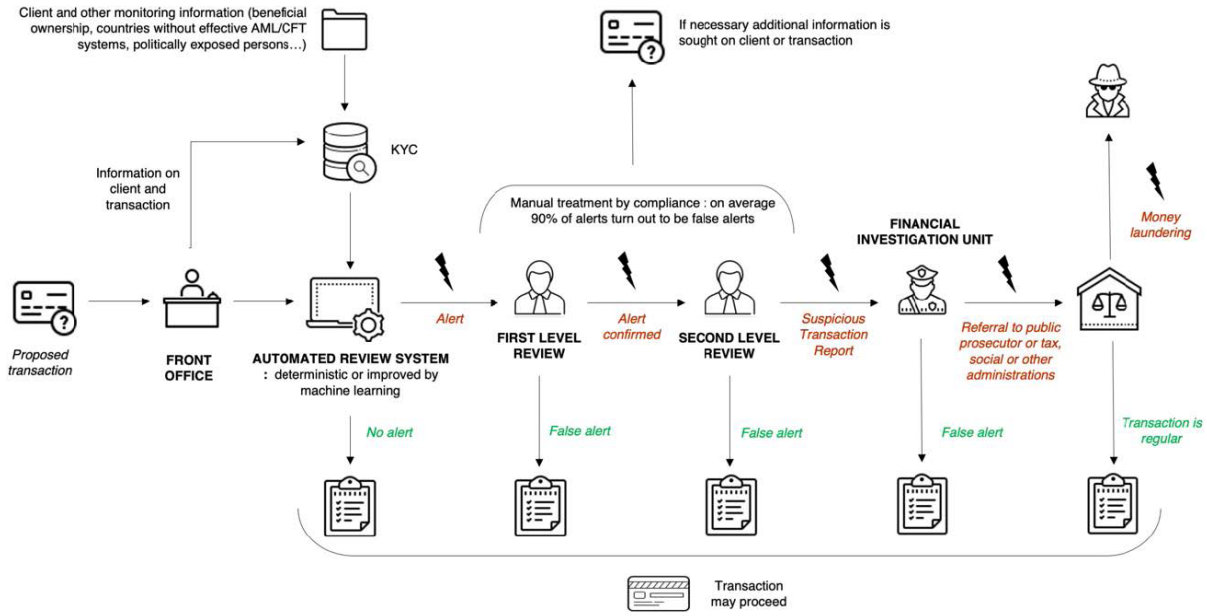

Image 1. Representation of the traditional AML process.[32]

The AI enabled AML Process

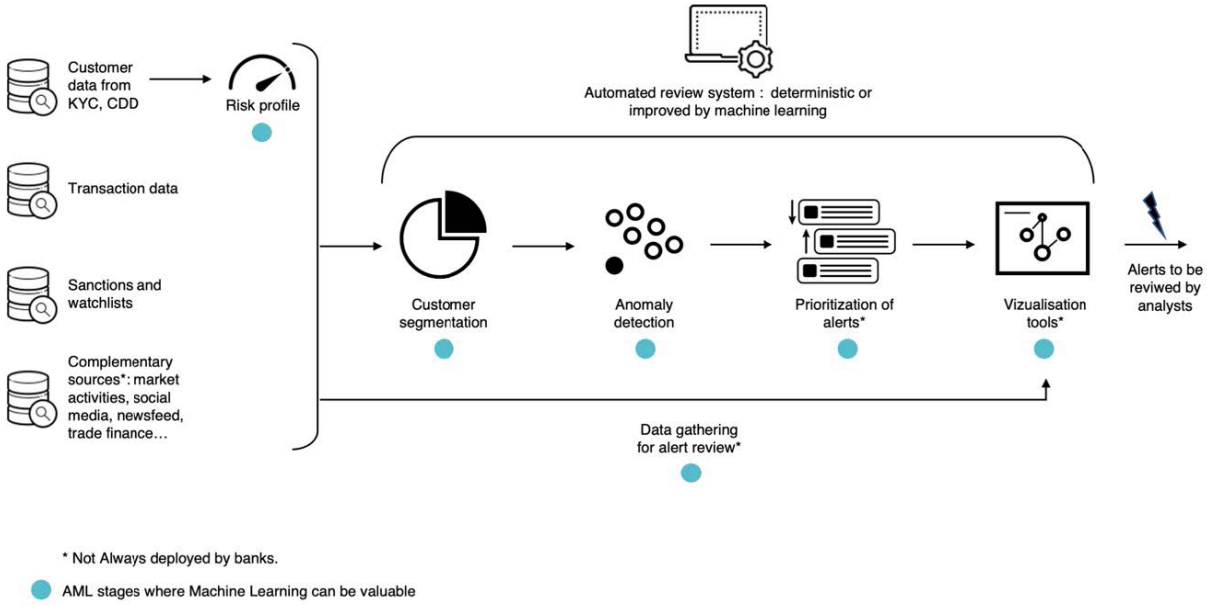

Image 2. Representation of the stages in which AI and machine learning can be used to improve the traditional AML process.[33]

32 Image credit: Astrid Bertrand, Winston Maxwell, Xavier Vamparys, "Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?", 2020, Telecom Paris Research Paper Series November 2020.

33 Image credit: Ibid.

Additionally, solutions such as APIs and DLT, data standardisation, and machine-readable regulations can assist regulated entities in reporting to supervisors and other competent authorities more efficiently. Alerts, report follow-ups, and other communications from supervisors, law enforcement, or other authorities to regulated organisations and their customers, as well as interactions among regulated entities and between them and their customers, can be streamlined through technological means.[34]

According to the FATF, technology-based solutions may even improve financial inclusion, provided they are deployed responsibly and through a risk-based approach.[35] New technologies must be adopted in a responsible, proportionate and risk-based approach manner, which maximises effectiveness gains whilst ensuring financial inclusion and the protection of underserved populations, data protection and privacy.[36]

The following sections explore what we found out (and what we could not) regarding this key proviso of responsible, risk-based deployment. Our fact-finding process was guided by the principle that confidence in the technology used in the financial sector is critical to a well-functioning society. A lack of confidence in these technologies could result in a loss of confidence in the financial system as a whole. Trust and confidence should be sought not only from those engaged in designing or deploying technology but also from those expected to use and be affected by it. As such, both experts and non-experts should have or be able to find basic but accurate information regarding the capabilities, risks and limitations of a given application in order to maintain a healthy level of informed trust in the system where those applications are deployed.

II. Standards for technology design, development, deployment and operation

In order to confirm how responsibly this technology is being developed and used, our inquiry centred on the key benefits and risks of relying on emerging technology, whether those developing and operating such technology were aware of such risks, and whether any safeguards or risk mitigation measures were in place or in contemplation. This chapter examines our findings regarding the surveyed emerging technology solutions' design, development, deployment and operation conditions.

We were fortunate to discuss these standards and conditions with several research participants. One of the financial institutions that develops its own financial technology in-house provided a comprehensive overview of its pipeline. They stated that the process is usually initiated by compliance personnel who request specific solutions to enhance their work processes. The developers then begin their work. The

34 FATF, "Opportunities and Challenges", p. 7.

35 FATF, "Opportunities and Challenges", p. 16.

36 FATF, "Opportunities and Challenges".

project team consists of business developers, data scientists, internal experts, and, on occasion, external experts such as the FIU or the police.[37] After determining the most appropriate type of machine learning for the task at hand, they model and test the results with different analysts to assess the generated alerts, gather and process relevant feedback, and iterate. Following a comprehensive risk assessment of operational, regulatory, and reputational risks, a formal DPIA assessment is performed, followed by a technical assessment focused on model validation. Then the approvals process begins, typically taking six months and requiring approval from two separate approving boards focused on model acceptance and financial crime risk, respectively. Finally, the project is turned over to IT in order for the new tool to be implemented and made live in the organisation. Furthermore, they expressed efforts to continuously improve and update existing models.

The majority of the remaining research participants provided only brief descriptions of their design, development and deployment pipelines. One financial institution stated in somewhat vague terms that legal issues and considerations are taken into account during the development stage and discussed with IT accordingly. Several FinTech companies described a collaborative design approach involving both their product team (which is constantly looking for ways to improve their offering) and existing clients (who frequently request new solutions for their problems). However, they did not disclose much more about how the process unfolds.

The remainder of our findings will be grouped under six overarching themes closely linked to responsible technology innovation. Each theme is presented in a Q&A format to improve readability.

1. Effectiveness & Reliability

Are emerging tech systems operating in a reliable manner, consistent with their intended purpose and without unforeseen or unintended consequences?

Overall, our research shows that the private sector believes the technology they develop or operate to be accurate and effective. The most commonly cited benefits of the technology included time and cost savings, risk reduction, revenue generation and commercial growth. Illustratively, one FinTech company described how their offering of digitised, machine-readable and queryable compliance regulations through an embedded API empowers financial institutions to do "more business, with more clients, in more countries". Using their product to confirm whether they are allowed to accept a new client or transaction is more cost-efficient than hiring a lawyer to obtain

37 We note that no external stakeholders from the NPO, human rights or data ethics sectors seem to be involved in this financial institution's development team, or in any other research participants'. This is further explored in Section II.

bespoke answers to their legal and compliance questions. It is likewise faster than reading through lengthy internal policies. Their clients' time is thus liberated to focus on revenue generation while their regulatory risk remains under control and "as close as possible to zero".

Every private sector interviewee stressed the benefits of their technology in the fight against financial crime and the improvement of compliance checks. One financial institution defined the financial institution's ML-based crime detection models as more efficient at detecting unusual behaviour linked to financial crime and better targeted, resulting in fewer false positives overwhelming the analysts.

Several FinTech companies framed their AI as an amplifier of human abilities, proposing that machines and humans excel at different tasks and resources should be allocated accordingly. "Never send a human to do a machine's job" and "shift human attention to areas where it can truly shine" were two decrees that stood out among several claims that AI is often misunderstood. AI is reportedly there to empower humans with its superior ability to assess probabilities and deal with complexity. We will return to this topic in Section II, Theme 5 - Human Oversight & Technical Competence.

One FinTech company highlighted how their technology's ability to extract insights from unused data could reduce de-risking by allowing financial institutions to benchmark risk profiles and take more nuanced views of correspondent financial institution relationships. They reason that many customers and correspondent banking institutions are inappropriately classed as "high-risk" and de-risked based solely on their location or size. With more data and actionable insights (such as benchmarks regarding the robustness of those customers' or correspondent baking institutions' compliance and due diligence systems), financial institutions will be more likely to accept those banking relationships, improving financial inclusion.

There was little disclosure of errors or inaccuracies. "We remove all the ambiguity" from the process, said one FinTech business, positing that if they could not offer 100% reliability, the customers would not rely on a digital solution. "The stakes are too high".

However, non-FinTech interviewees showed more scepticism regarding the precision associated with these tech-enabled compliance checks. One financial crime expert stated that customer profiles often lack essential information. Other researchers indicated that the technological solutions in use right now are blunter than people think, claiming for example that "the machine learning is still in the lab, not in production". Meanwhile, one financial institution claimed that the technology under discussion was not even that "emergent" ("it is already here"), while another contended this technology was not genuinely new or a panacea by any means. "Old challenges persist, and data quality remains an issue", said the latter.

Data quality was by far the most mentioned challenge to effectiveness and accuracy. One FinTech company conveyed a lack of reliable raw data sources. A financial crime expert expressed doubts that a single financial institution's data sets were large enough to enable real machine "learning", especially when combating terrorism financing, which is rare and does not have recurring typologies. A machine learning expert explained how that could result in overfitting[38] and spurious correlations.[39] NPOs seem to be especially vulnerable to these problems, given how small their data set is. We will explore this further in Section III of this report.

Data sharing was also mentioned as a related risk. One researcher contended that financial institutions needed to share data amongst themselves to set up more efficient AI systems, such as network graphs. However, this would raise cross-contamination risks. Hypothetically, if one customer were flagged as suspicious in financial institution A and financial institution B were able to see that, the customer would be locked out of financial institution B. Privacy-enhancing technologies to share data while keeping the results private, as well as public-private partnerships to pull more data from financial institutions, regulators and authorities and better understand criminal networks were discussed as potential - albeit not yet viable - solutions.

Apart from a general discussion about technical errors and inaccuracies, there was scarce acknowledgement of potential unintended consequences across most interviews. In some cases, interviewees did not even seem to grasp the concept or have meaningfully reflected on the wider socioeconomical impact of their technology. When asked whether they have any processes in place to assess the potential adverse impact of their products on human rights (e.g. regarding profiling and freedom from discrimination or similar), the majority of the interviewees did not even have a specific ethical review component in their design and development pipeline.

> Evaluating emerging tech systems' effectiveness in accomplishing a narrowly defined goal is not enough. Consideration of the technology's unintended impact

38 Overfitting is a term used to describe machine learning models that adjust too well to the training data, learning an excessive level of detail and noise that negatively impacts the model's performance on new data. The purpose of a machine learning model is to generalise patterns found in training data in order to accurately predict new data that has never been presented to the model. The size of the training data plays a critical role in overfitting. If there is insufficient data for a large number of features in the model, the model may see patterns that do not exist and become biased towards outliers. In a small data set, the weight of an outlier will be disproportional. As a result, the model will perform poorly with unseen data. Models that perform much better on the training data than on the test data are likely to be overfitted. For more, see: "Techniques And Pitfalls For ML Training With Small Data Sets — Trustbit". 2022. Trustbit. Available at: https://trustbit.tech/blog/2021/06/30/techniques-and-pitfalls-for-ml-training-with-small-data-sets. (Accessed 25 Apr 2022).

39 The appearance that two unrelated elements are causally related to one another can be further explored on "Beware Spurious Correlations". 2015. Harvard Business Review. Available at https://hbr.org/2015/06/beware-spurious-correlations. (Accessed 25 Apr 2022).

on other fundamental values such as privacy, fairness, absence of prejudice and freedom from bias is equally important. To illustrate the concept of effectiveness we support: we argue that, in order for a herbicide to be deemed effective, the producer must demonstrate not only the herbicide's ability to kill the target weeds but also its ability to do so without harming non-target plants, the soil, the person administering the product, and the environment in general.[40] Likewise, the adoption of emerging technologies for compliance purposes should be grounded on robust evidence that they are fit for their intended purposes and do not cause disproportionate unintended consequences. A technological system with a disproportionate impact on fundamental rights is ineffective.

Can the developers and operators of emerging technology demonstrably prove and measure the effectiveness and fitness for purpose of their technology through valid, credible and actionable benchmarks or metrics?

Although we had the opportunity to participate in several insightful discussions about the technology's benefits, success claims, and even a couple of case studies (which we cannot disclose here due to the report's anonymised nature), not many valid, measurable benchmarks or effectiveness metrics surfaced from the interviews.

When asked whether they would like to share any success metrics, most interviewees did not. Those who shared success metrics did not share the underlying data validating their assertions. For instance, one FinTech company claimed their product reduced the ratio of false positives by 20%, but we did not have the opportunity to examine this comparison's baseline. Another such declaration that they could screen names in a measure of milliseconds, compared to most financial institutions' process of minutes, was not backed up by any additional data.

To reap the benefits of any complex system or application, confidence in its safety and effectiveness is required. People drive cars, fly aeroplanes, take medicine, and ride amusement park rides because they trust that the tools, methods, and people controlling those products adhere to safety and effectiveness standards that contain the inherent risks to a manageable level, proportional to their objectives and benefits.[41] This requirement for confidence is vital for financial technology.

Some baseline conditions must be met in order to accurately assess effectiveness

40 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems", First Edition. (IEEE, 2019), p. 223.

41 The IEEE, "Ethically Aligned Design", p. 220.

> in a manner that builds confidence and mitigates the dangers associated with misinformed technology adoption and deployment. There should be credible metrics that convey concise and actionable information about the extent to which a particular application met or failed its objectives. Metrics should be derived using scientifically valid methods. Additionally, they should be generally understood and acknowledged as proof of effectiveness and adopted by a sufficient number of practitioners to enable comparison. Finally, the measures should be open to both professional and public scrutiny.[42]

If such effectiveness metrics do exist, who has access to them?

To the extent these exist, they seem to be kept internally, partially disclosed to prospective clients for marketing and business development purposes and, if needed, to regulators and other authorities. They are not released to non-experts or the general public, and no specific consumer-facing metrics (with a different level of granularity and detail) seem to be prepared.

In a partly related discussion about model validation data, one FinTech company indicated a cautious openness to the idea of sharing this internal data with the NPO sector. This position was an outlier. Data validation and system performance monitoring are further discussed in Section II, Theme 5 - Human Oversight & Technical Competence.

> As mentioned earlier in this report, confidence in the technology used in the financial sector is critical to a well-functioning society. A lack of confidence in these technologies could result in a loss of confidence in the financial system as a whole. Trust and confidence should be sought not only from those engaged in designing or deploying technology but also from those expected to use and be affected by it. As such, both experts and non-experts should be supplied with valid information regarding the possibilities and constraints of a given application. In fact, the most important objective for a clear measure of effectiveness should be that it is understandable to non-experts, including the general public.[43] These persons may lack a technical understanding of how technology or compliance operate but still deserve basic information and the power to make informed decisions.

42 The IEEE, "Ethically Aligned Design", p. 226.

43 The IEEE, "Ethically Aligned Design", p. 226.

Table 1. Recommendations for Effectiveness & Reliability		For
1.1.	Policymakers and standard-setters should support benchmarking exercises designed to provide valid, credible and accessible measurements of the effectiveness of financial technology deployed at each stage of the compliance process.	FATF Governments
1.2.	Technology developers should pursue credible metrics of their systems' efficacy, whether through involvement in benchmarking exercises or by undertaking their own validation studies. The creators should disclose their techniques and results in plain language comprehensible to both experts and non-experts, without exposing proprietary information.	FinTechs FIs
1.3.	Industry groups, researchers and other organisations should work together to produce metrics relevant to the effectiveness of compliance technology. These metrics should be designed in collaboration with representatives from the technology and legal fields, as well as representatives from underserved communities in the financial industry, including NPOs.	Compliance Industry

2. Fairness & Discrimination

Is the technology accessible, inclusive and free from bias?

We found that the private sector predominantly approaches problems concerning bias and profiling primarily through a model-centric perspective, emphasising the potential bias in the data used in their applications over the broader environment in which those applications are deployed. Studies suggest that dangers inherent in the broader technical system in which their application functions (which may include additional software components, data sources, and interfaces), as well as the wider social environment, are less likely to be recognised.[44]

Larger and more mature FinTech companies and financial institutions stated that fairness and bias compliance are reviewed before models go into production.

44 de Andrade, Norberto Nuno Gomes, and Verena Kontschieder, "AI Impact Assessment: A Policy Prototyping Experiment", 2021. Available at https://openloop.org/wp-content/uploads/2021/01/ AI_Impact_Assessment_A_Policy_Prototyping_Experiment.pdf (Accessed 25 May 2022).

Statistical controls are included to ensure staff is presented with unbiased selections and does not develop prejudices due to the AI systems they use. However, a smaller FinTech company in operation for 1-3 years notably claimed they were "too early in the process" to face serious risks of inadvertent bias, suggesting that start-ups and scale-ups do not address such considerations from the outset.

One FinTech company showed awareness of potential bias in their data sources. As providers of digitised regulatory content, they appeared conscious that the legal content they make accessible through their easy-to-use API is still written by lawyers at the end of the day. Lawyers will have a specific point of view informed by many factors, starting with their jurisdiction. A UK lawyer and a Venezuelan lawyer may differ in their analysis of local law. This business' plan to work around this issue relies on including a more diverse set of content writers over time.

Another FinTech company, in particular, highlighted the lightness, accessibility and anti-discrimination potential of their application as part of their unique selling point. They noted that most of the existing AML solutions on the market lead to inherent ethnic, religious and other biases commonly associated with something as simple as an applicant's name. They claim their phonetics-based name screening tool reduces the potential for bias linked to name commonality or ethnicity and that their cloud-based application is a particularly lean and accessible tool.

> With the growth of technological solutions to prevent and monitor (financial) crime, ethical concerns over the accessibility, inclusivity and fairness of AI become increasingly important. Despite the surveyed businesses' stated commitment to fairness, inclusivity and accessibility, we note that their understanding of bias is limited, and their commitment remains, in many cases, more theoretical than applied. Few businesses implemented concrete measures to promote or ensure their professed values. Smaller businesses, in particular, either lack or fail to devote adequate resources to address these issues and do not consider them mission-critical at the start of their journey.

Does the technology directly or indirectly result in unfair discrimination against any individuals, groups or communities?

Some of the risk profiling and fraud detection applications assessed, particularly those dealing with smaller data sets and relying on sensitive attributes (including business profile, gender, age, job status, income or location), may result in highly disparate

false-positive rates between specific categories of people and groups.[45] This possibility could lead to unequal and unfair access to financial services based on sensitive criteria, posing a risk of economic loss to mistakenly rejected applicants.

Several AI algorithms are known to reproduce the programme developers' conscious and unconscious biases. These biases are then applied at scale to unfairly target the financial activities of certain types of individuals or entities as suspicious, producing risk profiles and decisions that deny them access to certain financial products and services.[46] As the FATF states, special consideration should be awarded to neglected people and groups that may face exclusion due to cultural, political, or other factors.[47]

Nevertheless, our interviews did not show the technology developers or operators to have quantified such discriminatory effects or placed safeguards against all such risks. Discussions about the small size of the data for NPOS and the dangers of wrong decisions mediated by algorithms trained on small data sets did not reveal any concrete measures to address the issue.

The issue of unfair discrimination caused or exacerbated by technology is compounded by the fact that AML laws are, to some extent, discriminatory by design. A couple of interviewees remarked that the legal approach itself creates discrimination. While unavoidable discrimination can be justified - for instance, under European Union law - AML discrimination, in particular, has not truly been placed under the spotlight to determine whether such discrimination is justifiable. Although AI is supposed to be more accurate, our research did not uncover specific ways in which technology addresses and visibly reduces that discrimination.

> There are multiple and often subtle ways discrimination can occur through the deployment of technological solutions. Facial recognition is a widely used form of FinTech for performing ID checks. Automatic identity verification is contingent upon the quality of the camera used to take a selfie. By default, customers from lower socioeconomic backgrounds who cannot afford expensive phones will have poor image quality, making it more difficult for the algorithm to recognise data points and confirm the identification process. As a result, such technologies can raise additional hurdles and barriers for individuals from certain backgrounds.
>
> Another way technology can lead to discrimination is when an algorithm learns to use data points such as race, religion, and gender as risk indicators. When algorithms are trained on data that already contains bias - such as the assumption

45 See the discussion about overfitted machine learning models under Section II, Theme 1 - Effectiveness & Reliability.

46 FATF, "Opportunities and Challenges", p. 43

47 FATF, "Opportunities and Challenges", p. 43.

that certain minority communities are more likely to commit financial crimes - the algorithm will reproduce this bias when monitoring transactions and assigning risk scores. Singling out wholesale categories of customers traditionally regarded as high-risk (for instance, Islamic charities) to develop or improve models could prove highly problematic. Especially with machine learning and algorithms that use multiple data points to assign risk scores, many of which may not be clear to the compliance personnel tasked with reviewing the results.

Is the technology designed and operated to ensure fairness and financial inclusion?

Our findings suggest that accuracy and efficiency for compliance teams are more valued than fairness and financial inclusion outcomes. With one notable exception, fairness and inclusion did not seem to be part of the core business model of any of the interviewed participants from the private sector. However, one FinTech company articulated "the improvement of financial inclusion" alongside "the fight against financial crime" in their core business philosophy.

This FinTech company believes extracting value from unused data can allow typically underserved communities and financial players to prove the security and robustness of their systems beyond what their location or scale would typically indicate, resulting in a more accurate risk profile that may become more palatable to risk-averse financial institutions. They also mentioned that a couple of surveys across their client base revealed that, thanks to their technology's insights, some clients ended up not de-risking certain partners altogether, which opened new viable markets for them. However, they could not share more concrete data about this trend, which aligns with our findings on effectiveness metrics discussed in Section II, Theme 1 - Effectiveness & Reliability.

A research participant in another study we came across as part of our desk-based research mentioned potential measures to balance the accuracy and fairness considerations. These included a "fairness-aware model selection" that weighs the fairness score at any level of predictive accuracy and selects the model with the best fairness-accuracy trade-off.[48]

The potential for increased financial inclusion is one of the promises of emerging technologies. This promise is predicated on the assumption that technological solutions for compliance will make compliance easier for financial institutions while also lowering their compliance costs. As a result, instances of de-risking would be reduced, tipping the cost-benefit analysis of financial institutions in a

48 de Andrade and Kontschieder, "AI Impact Assessment".

way that improved financial inclusion.[49] Reduced compliance costs could benefit business relationships with correspondent banking institutions or clients operating in high-risk jurisdictions. If technologies were more sophisticated in monitoring and filtering transactions on the basis of more specific risk factors, entire jurisdictions or industries would not have to be rejected as they were previously with rule-based compliance practices.

While FinTech firms advocate for and promote more precise and inclusive compliance technologies, the question of whether these new technologies will result in increased financial inclusion remains unanswered. Apart from the issues of bias and discrimination previously discussed, the inclusion of marginalised or underserved communities is ultimately determined by the risk appetite of each financial institution. Even if compliance checks become less expensive, faster, and easier, financial inclusion could be elusive if larger financial institutions remain risk-averse. A proactive and shared attitude toward including and serving marginalised communities is needed to combat financial exclusion and de-risking.

Table 2. Recommendations for Fairness & Discrimination		For
2.1.	Financial institutions should avoid making technology a factor of exclusion. ID verification and other processes that require high-end equipment run the risk of excluding individuals based on their socioeconomic status or purchasing power. Viable alternatives should be provided.	FIs
2.2	Technology developers and procurers should assess not only a system's performance but also its outcomes and overall impact. Have the objectives of eliminating discrimination and minimising bias been properly integrated into the system's design and implementation? Have formal fairness standards been built and made explicit? Is there any evidence that the model has prevented discriminatory outcomes? Has the system's impact on affected individuals and groups been factored into the AI model?	FinTechs FIs

49 Woodsome and Ramachandran, "Fixing AML".

2.3.	Technology developers should actively monitor their products for discriminatory decisions in order to identify and mitigate bias. This will require additional effort to ensure that (i) the training data is not biased, (ii) algorithms that generate risk assessments are not based on categories such as race, gender, or proxies for these sensitive categories, and (iii) this process is continuously monitored. We recommend assigning this task to a designated data steward or human rights expert within the organisation.	FinTechs FIs
2.4.	Financial institutions should continuously monitor the use of AI in their compliance work. This requires both the oversight of potential discriminatory bias in daily compliance and the ability to report instances of discrimination. In line with our recommendation for technology developers, we recommend that financial institutions designate a specific member of the compliance team to receive and handle complaints on this topic, prevent bias on a proactive basis, and raise employee awareness.	FIs

3. Security & Data Protection

Do the emerging tech systems respect and protect the data subjects' privacy and ensure their data security?

The overwhelming majority of technology developers and operators answered this question positively. Those who did not, justified it by saying they do not have significant interaction with their customers' sensitive data, stating they were "more like systems auditors". Cybersecurity and privacy concerns seem to be taken rather seriously - even by start-ups - due to strict legal requirements such as the General Data Protection Regulation (GDPR).

Financial institutions noted that increased and ethical data sharing schemes between accredited institutions would be helpful. This ties in with the data sharing and data quality challenges discussed in Section II, Theme 1 - Effectiveness & Reliability.

Procedures for enhanced and secure data sharing between stakeholders were also discussed with one FinTech company whose business model centres on cryptographic protocols to share and get value from data across the financial services industry without exposing the underlying data. We emphasise that this FinTech company also

sought to engage and collaborate with stakeholders from the NPO and human rights sectors in the development of an upcoming prototype for AML/CFT compliance. We found such examples of collaboration between AML/CFT technology developers and the NPO sector quite rare, as we explore further in Section III of this report.

Financial institutions recognise privacy compliance as a critical issue. Due to the broad and complex regulatory framework that requires businesses to comply with the GDPR, all of our respondents made substantial efforts to establish functions within their organisations that explicitly monitor and address privacy concerns. This scenario indicates that clear and enforceable laws and regulations are critical when it comes to AI and ethics. They provide concrete and actionable tools and motivation for businesses to make ethical decisions surrounding technological developments.

Our research also showed that new technologies may present new possibilities for data sharing, in line with other studies highlighting the potential of distributed ledger technology for secure data storage and sharing.[50] A secure data sharing method might increase efficiency in compliance practices and reduce time and costs incurred. In order to improve transaction monitoring practices, the Netherlands is currently testing a platform for sharing transaction data. This initiative (Transactie Monitoring Nederland) is the result of a collaboration between four major Dutch financial institutions. One of the five pillars that structure this initiative is the responsible use of transaction monitoring models and oversight by a board of independent ethical advisors who advise on privacy and ethical data-sharing issues.

Do the data subjects have conditions to meaningfully understand and control how their data is being processed, including the analytics and algorithmic procedures used to analyse their data?

Some FinTech companies stated that customers did not need to be notified when they processed their data since the data was already publicly available.

One financial institution mentioned that their webpage displays only the minimal regulatory information that is legally required. Additional information regarding the models and rules they are running to process the customers' data is not shared. Moreover, they stated that any customer who sought to learn more about those elements could be flagged for suspicious behaviour. More on this topic in Section II, Theme 4 - Transparency & Explainability.

50 Woodsome and Ramachandran, "Fixing AML".

It appears reasonable to conclude that data subjects receive little more than the opportunity to review predefined terms and conditions and privacy policies designed to protect institutional interests. In an era where it is difficult to predict all the value and inferences that can be extracted from data, it is questionable whether the extent of information shared with data subjects is enough to ensure genuine agency over the use of their data.

Clients who use financial services share a lot of their personal data. Personal data is submitted during the onboarding process and also extracted from customer behaviour on a continuous basis. Under the GDPR, financial institutions may use this data for security and compliance purposes so long as the intention is to prevent financial crime. However, data agency and ownership issues should extend beyond a pro forma adherence to the GDPR. If individuals are constantly required to make decisions regarding data in such a way that generates data fatigue, or if they lack the knowledge needed to determine when it is safe, necessary or beneficial to share their data, the consent they provide for the processing of their data will not be informed or valuable.

Within the broader literature on data ownership and agency, several models to prevent the loss of data ownership are being discussed. Suggestions such as data commons and data trusts,[51] for instance, could be considered for data sharing for compliance. Health care, which has been consistently focused on ethical risk mitigation for at least five decades, can also be a source of inspiration for leadership in the compliance sector. Medical ethicists, health care practitioners, regulators, and lawyers have all looked into what constitutes privacy, self-determination, and informed consent for medical procedures.
Their insights can be applied to various ethical challenges involving customer data privacy and control in the financial sector.[52]

51 In these initiatives, the data is managed by a trustee or through communal forms of decision-making, providing an alternative to binary decisions (accept/reject all) on data ownership. Mills, Stuart, "Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership", September 24, 2019. Available at SSRN: https://ssrn.com/abstract=3437936 (Accessed 25 May 2022); De Lange, Michiel, "The right to the datafied city: Interfacing the urban data commons.", in: The right to the smart city. eds. Cardullo, Paolo, Cesare Di Feliciantonio, and Rob Kitchin (Emerald Group Publishing, 2019); Delacroix, Sylvie, and Neil D. Lawrence, "Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance." International data privacy law 9. 4 (2019), p. 236-252.

52 For instance, in health care, one of the most important ways to show respect for patients is to treat them only after they have given their informed consent, which abhors, at a minimum, lies, manipulation, or communications in words the patient does not understand, such as impenetrable legalese or Latin medical terms. The same kinds of principles can be applied to the collection, use, and sharing of the personal data of financial institutions' customers. One simple lesson to draw from health care is to ensure that consumers are not just told about how their data is used, but also that they are informed early on and in a way that enables comprehension (for example, by not burying the information in an extensive legal document that will be skipped over due to decision fatigue). For more, see Harvard Business Review, "A Practical Guide To Building Ethical AI.", 2020. Available at https://hbr.org/2020/10/a-practical-guide-to-building-ethical-ai. (Accessed 25 April 2022).

Table 3. Recommendations for Security & Data Protection		For
3.1.	Businesses should deconstruct broad ethical notions like privacy, bias, and explainability into infrastructures, processes, and practices that fulfil those principles and continuously consider ethical initiatives and new developments for data protection and sharing.	FinTechs FIs
3.2	Financial institutions, regulators and other bodies considering innovations such as data sharing across organisations should do so in consultation with privacy experts and with the knowledge of the affected data subjects.	FIs FinTechs Governments Supervisors

4. Transparency & Explainability

Is there sufficient disclosure and transparency regarding the use of emerging technology, such that impacted individuals can understand when and how they are affected by it?

Apart from the limited amount of regulation-required information shared with data subjects by developers and operators, as detailed in Section II, Theme 3 - Security & Data Protection, several interviews conveyed the message that the individuals whose data is processed through the use of emerging technologies remain, for the most part, in the dark.

"Much of what happens is not visible to the client", explained one financial institution. To avoid tip-off, the client may receive additional information requests from the financial institution without ever being informed that an FIU has been contacted.

The amount of information technology developers provide to the financial institutions licensing their technology varies. We were unable to verify what information is provided to regulators. One FinTech company described how holding certain regulatory licences and incorporating monitoring and oversight committees as part of their governance model tends to decrease the number of inquiries concerning their product's inner workings.

More access to information about emerging technologies' actual use and outcomes is critical. Those directly or indirectly affected by this technology (including, sometimes, the general public), have a vested interest in the effective functioning of the financial system. Without transparency, there is no way to trust or verify that a given decision mediated by emerging technology can be explained or, if necessary, corrected. There is no basis to confirm that these applications adhere

to normative or legal standards and produce fair results. There are no means to ensure that those engaged in the design, development, deployment, operation and validation of the effectiveness of these applications can be held accountable for negative outcomes.

Naturally, public access to all information on the operation and results of this technology is not desirable. Nevertheless, a deliberate and careful assessment of who should have access to what information in a way that still fosters informed trust should be required. Concerns related to data privacy, proprietary or commercial stakes, public policy, or even security interests (including concerns about gaming and adversarial attacks) may be legitimate. However, they should not be used, without visible efforts to balance competing interests, as a blanket excuse for not adhering to due process, transparency, or accountability standards.[53]

Are the basis of decisions made through tech augmentation or automated decision-making traceable, understandable and explainable from the perspective of (i) those developing the technology, (ii) those operating it, and (iii) those affected by it?

Unsurprisingly - given the existing requirements for financial services technology and the nature of the technology developed by the stakeholders who agreed to participate in our study - every interviewee reiterated that the technology was completely explainable and did not involve black-box algorithms. Despite our attempts to contact developers of what appeared to be more complex and less explainable models, they declined to participate in this study.

Every research participant stated that their application allows operators to understand how a decision was made and why a transaction was flagged. "We have a full explanation with a straight mathematical formula", mentioned one FinTech business. "There are audit records that show precisely what the query was, what data sources were used. The client can generate a report to get that information", said another. Suppose a client deviates from the algorithmically-generated decision due to their own risk appetite. In that case, it is possible to pinpoint the different elements behind the algorithm's decision and the client's overrule thereof.

When asked whether the audit trail revealed instances of technology intermediation, however, at least one FinTech company stated that it did not. For instance, a report would disclose the specific sources found on the dark web containing information that affected the risk profile of a prospective client. However, if some of those sources were parsed or processed using NLP or fuzzy logic rules, these technological steps would not be highlighted in the report. The business reasoned that such disclosure was

53 The IEEE, "Ethically Aligned Design", p. 248.

unnecessary because "the machine is not creating the data that triggers the alert, it just retrieves it".

By comparison, the responses regarding the explainability of decisions vis-à-vis those affected by such decisions were more ambiguous. Technology developers seem to focus predominantly on ensuring automated decisions are explainable to operators, regulators and supervisors. Not much heed is paid to explaining the rationale behind decisions to the subjects affected by those decisions. A need for secrecy was frequently depicted as a necessary precaution against strategic classification and other risks.

Many private sector respondents expressed the fear that if algorithms become more transparent and explainable they will also be less efficient, and such knowledge will be used to "game the system" and circumvent compliance rules. Non-private sector participants debated the real extent to which financial service users can strategically adapt to classifications, even if known.

Although there is hearsay of people gathering in online forums to share information on how to game certain financial institutions' account opening systems, how substantial or anecdotal is this evidence and the risk it would present? In the case of terrorism financing, there are often limited ways of transferring money to organisations or individuals. Usually, transfers are made through informal banking systems or through normal banking behaviour that can only be classified as terrorism financing in retrospect. As such, it is difficult to predict that more transparency around compliance will have any significant effect on terrorism financing practices.

In summary, we were unable to validate the seriousness of this risk or the true extent of the need for secrecy to avoid gaming and strategic classification. Although secrecy needs have existed in this area independent of technology use, their use as a strategy to evade demands for transparency about technology use is noteworthy. The extent to which secrecy serves legitimate aims, compared to the extent to which it may be perpetuating the use of inaccurate systems that may thus remain unscrutinised and uncorrected, remains an open question.

> Clearly, there is some perceived tension between goals such as transparency and explainability, on the one hand, and effectiveness and system performance, on the other. The chief concern seems to be that, if the decision subjects know too much about the inner workings of the systems making decisions about them, they will use this knowledge to game that system. However, this scenario assumes the existence of a perfect system that should be protected from gaming at all costs. If the system is flawed - for instance, if it relies on inaccurate proxies to mark suspicious behaviour, causing a machine to learn wrong patterns - then that system will yield inaccurate and unfair results. So long as the system remains unscrutinised,

no progress will be made to improve it. This scenario does not serve the objectives of effectiveness and system performance either.

Once again, we do not argue for unfettered public access to all critical information about a system. However, some level of transparency and explainability is important, and providing it to different stakeholders would produce multiple beneficial results. Operators need to understand the systems' processes and input data so that they may challenge a decision produced by these systems when appropriate. Decision subjects need and deserve to know the basis and rationale for the decisions that impact their access to financial services. They are the proverbial canaries in the coal mine, the ones most sensitive to potential and concealed issues that directly impact their rights. Cutting them out of the loop is not guaranteed to help keep the systems impervious to gaming. Furthermore, it removes one possible route to improve those systems, which may be sorely needed considering how scarce the metrics for the effectiveness of those systems are in the first place.

Table 4. Recommendations for Transparency & Explainability		For
4.1.	The FATF, as well as regional and national regulators, should facilitate dialogue among several stakeholder groups, including those involved in the technology's design, development, deployment, operation and effectiveness validation, those with specialised knowledge in tech ethics, compliance and the law, but likewise those who may be directly or indirectly affected by the technology's results, including marginalised communities and the general public in some instances.	FATF Governments
4.2	Policymakers should not allow competing concerns such as data privacy, trade secrets, public policy, or even security interests to fully override the need to disclose information essential to verifying standards of effectiveness, fairness and safety. Efforts to balance competing interests in a proportional way should be made.	Governments

4.3	Developers and procurers of FinTech solutions should categorise different types of relevant information into high-level categories and determine which types of information may be disclosed to different stakeholders regarding the design, operation and results of a given system. Information disclosure should be tailored to each stakeholder.[54]	FinTechs FIs
4.4	For sensitive information which should not be widely available for legitimate reasons, an additional independent figure such as a public interest custodian could be created and empowered to request and receive sensitive information relevant to certain groups or the general public.[55]	Governments

5. Human Oversight & Technical Competence

Is the technology subject to human oversight and control?

The overwhelming response was that human oversight existed at all critical stages of the process, with human control over the final decisions.

"Humans create the rules", mentioned one FinTech company, "the machinery is in how you read those rules alongside each other, mesh them together, and what output you get". Another FinTech business described humans as "an under-utilised resource", suggesting machines should do "the grunt work" and save humans for processes machines cannot do well. Other FinTech businesses characterised their systems' role as a human supplement, enhancing human abilities and transforming them into superheroes, combating financial crime while saving their organisations time and money.

One financial institution explained how AI creates alerts, and human analysts conduct a manual assessment of those alerts. "There is no 100% AI/ML-based risk assessment", no fully automated decision-making. "We still need humans to make decisions about humans, investigate, make calls, visit premises", said another financial institution,

54 The IEEE in "Ethically Aligned Design", p. 245 provides a helpful taxonomy of such high-level categories: nontechnical procedural information regarding the employment and development of a given application; information regarding data involved in the development, training, and operation of the system; information concerning a system's effectiveness/performance; information about the formal models that the system relies on; and information that serves to explain a system's general logic or specific outputs. Not all categories of information are needed (or even helpful) for all stakeholders, but a framework in place for category sharing should be developed.

55 The IEEE, "Ethically Aligned Design", p. 245.

adding, "but we are still in the process of realising what the optimal level of human involvement is".

> Human actors must be tasked with identifying, assessing and mitigating the risks stemming from reliance on emerging technologies. In order to avoid uncertainty and apprehension about the use of emerging technologies in the compliance sector, the general public must have confidence that the developers and operators of such technologies are developing them responsibly and overseeing their use with due care. The appropriate level of human involvement must be clearly defined and implemented. Without it, confidence in financial technology and the financial sector itself is hard to maintain.

What is the level and quality of human intervention during (i) the conception and design of algorithmic systems and (ii) the validation or reconsideration of algorithmically-derived decisions?

Despite assertions that human control is critical, neither developers nor deployers of compliance technology painted a thorough picture of the conditions surrounding human control over algorithmic-generated decisions.

The broad strokes of the "human hand" present during the set-up of some of these systems were shared. For instance, in the case of a surveyed API displaying actionable, digitised legal content, lawyers were involved in producing the content that was then subjected to decision trees by programmers and displayed in an easy-to-use client interface. In the case of surveyed algorithmic systems, we understand that humans define the problem to address, the decision criteria, the training data, sensitivity thresholds, and so forth. Humans then monitor the tests and audits, assign priorities to detected errors and biases, and other such (highly determinant) tasks.

In short, humans are moving the needle in several ways during the setup of these systems. They are also potentially embedding their own bias onto systems lauded for their purported neutrality, which presents the risks discussed in Section II, Theme 2 - Fairness & Discrimination.

However, the factors influencing human control over the validation or reconsideration of algorithmic-made decisions were less clear. For example, compliance officers base their decision on the type of alert generated by the system. Based on the type of alert, the compliance officers can make an immediate decision or escalate the issue within their department. One respondent indicated that, in the case of terrorism financing, these would usually be high-priority decisions taken by a broader team. Nevertheless, we could not find a consistent policy on ensuring human oversight across organisations.

Some observations shared by interviewees suggest that compliance analysts are often young graduates who received very theoretical knowledge, have not yet had their knowledge tested by real-world conditions, and are unlikely to expend extra time or effort gathering additional sources to judge the accuracy of algorithmic-made decisions. These observations are largely anecdotal. Are the levels of expertise and ability of the agents responsible for this human control and validation actively monitored?

We were unable to map out critical elements pertaining to human control over the validation or reconsideration of technologically-enabled alerts. Factors such as the amount of time and other information and sources available to the decision-maker, the amount of training received, the level of independence, the plurality of points of view at play, and the participation of the affected party would be extremely relevant in determining how consequential the level of human control over the machines they operate is. As such, fundamental questions remain. Can humans meaningfully challenge machine-made decisions? How often does it happen, and to what degree of success?

Operators of artificially intelligent systems may grow less willing - or perhaps unable - to challenge decisions or predictions made by algorithms. They will not always be aware of the sources, accuracy, and uncertainty inherent in AI applications. Even if systems leave a clear record of the processes taken to arrive at the current decision, operators may lack access to them or the specialised knowledge needed to understand them.

Recent literature indicates that the emphasis on human oversight might result in a false sense of security while changing little about the fundamental issues with the relevant tools.[56] Furthermore, humans are known to be susceptible to a type of cognitive bias known as "anchoring", an undue reliance on a single piece of information at the outset of a task.[57] This phenomenon would increase the likelihood that the human agents tasked with reviewing and challenging algorithmic-generated alerts, for example, would place excessive trust on the accuracy of the algorithm that created the alert and switch off their critical thinking as a result. In those cases, is human control achieved?

56 Green, Ben, "The Flaws of Policies Requiring Human Oversight of Government Algorithms." Computer Law & Security Review, no:45 (2022).

57 The IEEE, "Ethically Aligned Design", p. 220.

Do developers specify the knowledge and expertise necessary for their systems' safe and successful operation, and are those requirements adhered to by operators?

As far as we were able to determine, the FinTech businesses developing the technology surveyed in this report do not set minimum technological literacy standards for the technology operators. Some rely mostly on a training manual for their systems while others rely on user feedback to surface any operator difficulties.

Conversely, financial institutions claim that the (potentially non-technologically trained) human officers using the technology are ultimately responsible for interpreting the results correctly and making appropriate decisions. "They cannot blame the technology. They are the ones responsible for spotting any faults in the technology." More on this in Section II, Theme 6 - Accountability & Contestability.

Discussions with non-private sector interviewees also highlighted the concern that, by and large, operators are not held to specific competence standards. Users should understand how the systems they operate make decisions, the information and logic they use, and the consequences of those decisions. Creators of AI applications, in particular, should actively ensure that technology users have the knowledge, experience, and skill necessary to use their applications safely and effectively, towards their intended goals, and with the ability to overrule the application when needed.[58] If the results cannot be thoroughly contested and challenged, there is human involvement but not human control. The premise that this technology is simply a human aid falls by the wayside.

> Confidence in the competence and skill of technology operators is a core pillar of informed trust in a technical system, particularly one with the potential to significantly affect people's outcomes. We entrust surgeons and pilots with technical tasks because we know they have the education, skills, and training required to use complex tools and machinery, and to do their jobs properly. We know these operators have fulfilled stringent professional and scientific certification criteria before being licensed to enter the operating room or cockpit.[59] This well-informed trust in operator competence is what allows us to be comfortable in their hands. The inexistence of detailed competence criteria for operators in the AML/CFT setting makes it difficult to trust emerging technologies in the compliance sector.
>
> We must have reasonable grounds to believe that those operating technical systems have the skill and knowledge required to fully understand the conditions for effectively operating such systems. Where AI is involved, this requires knowing and understanding the data on which algorithms were trained, the data to which algorithms are applied, and how those elements influence the results they yield.

58 The IEEE, "Ethically Aligned Design", p. 32.

59 The IEEE, "Ethically Aligned Design", p. 231.

Table 5. Recommendations for Human Oversight & Technical Competence		For
5.1.	Policymakers should strive to build trust in emerging technology with the potential to determine people's abilities to transact and do business is essential. This requires clear and concise standards and best practices for two sets of agents: technology creators and technology operators.	Governments
5.2	Technology designers and developers must define the level of expertise and type of conditions needed for the systems' deployment and operation in a safe, ethical, and effective manner. A description of the dangers arising from the failure to meet those standards should be included in such guidance. The guidance should be recorded in a way that is both accessible and clear to professionals as well as the general public.	FinTechs FIs
5.3	Technology procurers and deployers should verify that their workforce meets the standards for competent operation.	FIs
5.4	Technology operators must commit to following such standards and guidance in accordance with all other applicable legal, ethical, and professional criteria.	FIs
5.5	Technology designers and developers of these systems should include safeguards against the inept operation of their systems. Depending on the context, operators could be issued notifications and warnings if concerning patterns of use are identified; access to functionality could be restricted based on the operator's level of expertise; the system could even be deactivated in potentially high-risk conditions, among others.[60]	FinTechs FIs

60 The IEEE, "Ethically Aligned Design", p. 235.

6. Accountability & Contestability

Are the parties responsible for the different stages of the tech pipeline identifiable and accountable for the outcomes of the systems they took part in designing or operating?

Our attempt to answer this question was inconclusive. Even the standards for monitoring system performance vary widely across organisations. Some FinTech companies have independent oversight committees responsible for issuing guidance on how well they are achieving and balancing competing objectives. Others have model validation tests performed and released quarterly. One financial institution with significantly advanced ML-based crime detection and risk profiling applications does not, to our understanding, have any internal responsibility procedures in place to address unintended harm caused by their products.

> The information we gathered is concerning. The possibility of assigning responsibility among the agents involved in creating and operating a system is a cornerstone for informed trust in that system and a key deterrent against shoddy design, haphazard adoption, and improper use of technology. The question "who is accountable" must have a clear and finite answer. If the answer is "no one" or "everyone", the result is the same - there is no accountability - and it is ill-advised to trust a system that produces outcomes for which no one is accountable.[61]

In the event of errors or unintended consequences, is it possible to assign culpability to designers, manufacturers or operators of emerging tech systems? How is the legal responsibility apportioned between them?

As mentioned in Section II, Theme 5 - Human Oversight & Technical Competence, one financial institution that develops its own compliance technology in-house expressed its view that the human officers using the technology are ultimately responsible for interpreting the results correctly and making appropriate decisions. "They cannot blame the technology. They are the ones responsible for spotting any faults in the technology." Other participants reiterated the basic rule of thumb that AI should analyse the data and humans should interpret it.

> Considering our findings regarding the standards for technical competence in Section II, Theme 5 - Human Oversight and Competence, the potential for failure inherent in this approach (i.e. the view that "humans cannot blame the technology,

61 The IEEE, "Ethically Aligned Design", p. 238.

they bear the responsibility for spotting any problems caused by it") is concerning. It also appears that the "blame game" which typically plays out in discussions about the cause of unintended consequences of AML/CFT measures (i.e. shifting the blame between the FATF, the regulators and the financial institutions), has been levelled up by technology. In the case of technological failure, should we blame the algorithm, the humans who created the algorithm, or the humans who should have spot-checked and challenged the algorithm?
For example, if a compliance officer wrongfully rejects or terminates a relationship with a customer (or an entire customer segment) because the officer incorrectly labelled such customers as high-risk, relying in part on an AI-powered risk profiling tool, who is responsible for the negative impact on that customer's life and business? Is it the tool designer, the individual who chose the data on which the algorithm was trained, the individual who determined how the model's effectiveness would be measured, the specialists who offered training to the compliance officer, or the officer?

In cases where the developers and the technology operators are different, we did not receive detailed feedback on how the legal responsibility is apportioned. One FinTech company shared their expectation that technical issues in the software are their responsibility. In contrast, mistakes caused by their clients' filtering choices or bespoke rules would be the clients' responsibility. However, based on our interviews with FinTech representatives, we could not determine whether these matters are consistently set out in the software licensing agreements and agreed upon between all relevant parties. Likewise, we could not determine whether a potentially impacted individual will have access to this information.

Can the rationale for decisions made through emerging tech-powered means be challenged, internally or externally? Are there timely and actionable ways to contest and dispute the process used to reach that decision or its outcomes?

Our research did not uncover any concrete procedures for contesting these decisions. Even when a technologically-enabled choice substantially impacts a person or group, the channels for challenging it are not readily apparent or feasible.

One FinTech company explained how a dissatisfied client could contact their customer support system, which could, in turn, contact the development team if there is a recurring data issue that requires software alteration. One financial institution mentioned that clients could request their client file and confirm how the financial institution processed their data from a GDPR perspective. Is this enough?

A different financial institution explained how different consequences apply to different issues. If an account is determined (by them) to have been used in a fraudulent manner, it will be closed, and the client will be removed from the system without the

ability to appeal the decision or reactivate the account. They described a zero-tolerance policy for "actual misconduct" (although the "actuality" of any misconduct which the accused cannot defend against or appeal is debatable). In contrast, if an account is merely flagged for suspicious behaviour and the client fails to answer requests for further information for some time, the account will be closed preventatively. However, the client could remedy the issue and reinstate their account in the future.

Guarantees that no mistakes will ever be made are not feasible nor required. However, proper methods for addressing and resolving those mistakes, should they occur, are needed to maintain informed trust in a system. A framework that lays out who is responsible for what, who has recourse to which corrective actions and - just as important - what information will be disclosed to enable problem-solving procedures. Meaningful audit of the basis on which decisions were made - including, when relevant, the technological processes behind those decisions - is needed to cultivate a culture of accountability. The opacity resulting from the complex interplay of algorithms, input data and code, coupled with the diffuseness of responsibility along the compliance chain, could prove a dangerous combination for the ability to assert one's rights.

Although not strictly connected to the AML/CFT setting, legal cases where the black-boxed nature of AI-powered recidivism algorithms used in the legal system made it impossible to challenge and seek redress for alleged injustices[62] may serve as a powerful omen. Recent lawsuits against a database that categorised an individual as connected to terrorism without any legal process or ruling (resulting in the termination of his banking relationships),[63] as well as legal challenges to mass data retention and the use of self-learning algorithms to detect presumptively suspicious behaviour typically linked to terrorism (with potential spillover

62 The IEEE, "Ethically Aligned Design", p. 241 highlights the dangers of the inability to interrogate AI tools in the legal system. "In 2013, Eric Loomis was arrested for a drive-by shooting in La Crosse, Wisconsin. No one was hit, but Loomis faced prison time. Loomis denied involvement in the shooting, but waived his right to trial and entered a guilty plea to two of the less severe offences with which he was charged: attempting to flee a traffic officer and operating a motor vehicle without the owner's consent. The judge sentenced him to six years in prison, saying he was "high risk". The judge based this conclusion, in part, on the risk assessment score given by Compas, a secret and privately held algorithmic tool used routinely by the Wisconsin Department of Corrections. On appeal, Loomis made three major arguments, two focused on accountability. First, the tool's proprietary nature—the underlying code was not made available to the defence—made it impossible to test its scientific validity. Second, the tool inappropriately considered gender in making its determination. A unanimous Wisconsin Supreme Court ruled against Loomis on both arguments. The court reasoned that knowing the inputs and output of the tool, and having access to validating studies of the tool's accuracy, were sufficient to prevent infringement of Loomis' due process. Regarding the use of gender—a protected class in the United States—the court said he did not show that there was a reliance on gender in making the output or sentencing decision."

63 For more information on the World Database lawsuit, see Webb, Tom, "Former Guantanamo Inmate Sues Refinitiv Over Global Risk Database." Globaldatareview.com, 2022. Available at https://globaldatareview.com/data-privacy/former-guantanamo-inmate-sues-refinitiv-over-global-risk-database. (Accessed 20 Apr 2022).

effects in the financial compliance arena),[64] may also foreshadow what could be coming for the developers and operators of financial technology deployed in the compliance system.

Table 6. Recommendations for Accountability & Contestability		For
6.1.	Technology developers should define responsibility levels for all parties involved in the use of their technology, including the potential subsequent liabilities of those who will be operating the systems they build.	FinTechs FIs
6.2	Technology licensing contracts should include contractual terms allocating responsibility for different issues that could stem from using the licensed technology.	FinTechs FIs
6.3	Technology developers and deployers should understand their responsibilities for negative outcomes and how they could be held accountable. They should also put in place or be open to internal oversight procedures and investigations required to allocate responsibility for outcomes generated or mediated by emerging technologies.	FinTechs FIs
6.4	Financial institutions should inform individuals adversely impacted by applications reliant on emerging technologies of the impact of such technologies on their outcomes. These individuals should have avenues to appeal or dispute resolution methods settled by competent human agents. In order to identify and challenge any issues, they should be provided access to basic information regarding the functions of those involved in the outcome they seek to challenge.	FIs

64 For more information on the case against Directive (EU) 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (in short: PNR Directive) and its compatibility with EU primary law, see Peers, Steve, "On Flights, Rock Concerts And The Needle In A Haystack: A Report From The Court Of Justice Of The European Union'S Oral Hearing On The PNR Directive." Eulawanalysis.blogspot.com, 2021. Available at http://eulawanalysis.blogspot.com/2021/09/on-flights-rock-concerts-and-needle-in.html. (Accessed 22 Apr 2022).

6.5	Those conducting investigations or audits involving technology applied in the compliance system should consider all human agents involved in the design, development, procurement, deployment and operation of such technology and assign responsibility accordingly.	Supervisors

III. Impact on the NPO sector

Prior ECNL research has shown that financial institutions' AML/CFT practices have a negative impact on the nonprofit sector. Even before financial institutions incorporated emerging technologies into their compliance workflows, there was already evidence that the entire sector was being tarred with the same brush and deemed problematic based on the misconduct of only a few agents.[65] Examples of this generalisation include the fact that NPOs:

- typically take longer to be accepted as financial institution customers and to get their transactions processed;
- are often unaware and uninformed about the systemic drivers behind many financial institutions' decisions that impact them, including decisions to close their accounts or reject their transactions without explanation;
- are disproportionately affected by their size, with smaller organisations suffering greater harm than larger ones and without remedies available to them;
- are ill-equipped to cope with financial institution's extended due diligence requirements, a difficulty compounded by the smaller size of certain organisations; and
- tend to seek their own solutions for the problems they face with their financial institutions, resulting in one-off rather than systemic solutions, even for sector-wide issues.

The most recent ECNL research shows that some of these issues spill over when emerging technology is layered on top of traditional practices for NPOs. In contrast, other issues might be improved through machine learning and more advanced systems for compliance.

65 ECNL and Human Security Collective, "Understanding the drivers"

Are NPOs treated as a specific customer segment?

Typically, financial institutions determine suspicious customers or transactions after completing customers' due diligence (CDD) during the onboarding stage.[66] They research, discuss and determine their prospective customers' expected transactions and activities before opening a new customer account. During this exercise, some financial institutions do not treat NPOs as a separate customer segment, treating them instead as any other business customer. However, some financial institutions view the NPO sector as higher risk and perform enhanced due diligence on all NPOs as a result.

One financial institution introduced a "segmented" approach for NPOs, including additional CDD requirements and distinguishing between local sports/cultural/music NPOs and those with an international profile. The latter is deemed to be higher risk. This financial institution also uses an "expected transaction profiling" tool for NPOs which generates alerts based on abnormal transaction patterns. These alerts are then investigated more closely.

Several financial institutions and researchers explained that external requirements dictate their treatment of NPOs. Some participants commented that NPOs are high-risk customers subjected to enhanced due diligence under local regulations. Others pointed to external sources identifying NPOs as more vulnerable to financial crime. In general, NPOs appear to be considered high-risk for potential terrorism financing in the same way that cash-intensive businesses are deemed high-risk for money laundering.

Notably, one of the researchers we interviewed commented that they had detected some bias against NPOs in a financial institution where they previously worked. These issues seem to stem from the placement of all NPOs in the high-risk customer category.

Treating NPOs customers (as a whole) as higher risk customers represents a flawed interpretation of AML/CFT requirements as well as the absence of a risk-based approach.[67] According to the European Banking Authority, de-risking of entire categories of customers without due consideration of the individual customers' risk profile can be unwarranted and a sign of ineffective AML/CFT risk management.[68] The possibility that this flawed approach will permeate the design and development of new technologies is especially worrisome. Due to the difficulties in challenging tech-based decisions

66 See També, "Unintended consequences".

67 See FATF, "High level Synopsis".

68 European Banking Authority (EBA), Opinion of the European Banking Authority on 'de-risking' (January 2022). Available at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf (Accessed 29 April 2022)

(as described in Section II, Theme 6 - Accountability & Contestability), technology would exacerbate and cement the negative impact of flawed AML/CFT measures on the nonprofit sector.

Our findings also indicate that institutional approaches sometimes vary when it comes to identifying NPOs as a specific segment of the customer base, and are unlikely to converge on the basis of technological advancements.

Although a few financial institutions identify NPOs as a separate group, based on distinctive customer features and transaction data, others do not have specific procedures developed for NPOs (in contrast to procedures developed for their customers in specific industries such as gambling and cryptocurrency) because they do not have enough NPO clients to justify such efforts. FinTech business respondents did not distinguish between different types of customers either, noting the group of NPO clients was not significant enough in size.

As they represent such a small group outside of the target demographic for most businesses, NPOs are unlikely to receive bespoke treatment. They are unlikely to be awarded a set of rules and procedures addressing their systemic issues. Even if emerging technologies could provide such solutions, businesses are not allocating resources to designing them with the NPO sector in mind. Some businesses even stated it is easier to perform due diligence on their NPO clients (which are few and far between and all local) through manual checks performed by humans.

Moreover, in some cases, large NPOs have their own account manager and, therefore, someone to talk to in case of a problem. Smaller organisations have difficulties speaking to someone if they encounter an issue.

Although some institutions argue that better machine learning might solve the issues faced by NPOs, in-depth knowledge of how NPOs operate is often missing. Despite the promise of AI and emerging technology, it seems financial institutions are unlikely to change their risk appetite or attitude towards NPOs. The rule-based approach is unlikely to completely disappear anytime soon, leaving de-risking as the only current consistent approach to NPOs. When NPOs are not distinguished from the general customer base, it remains unclear how the "general" technology approach could account for the NPO-specific issues, such as the bias described above.

What is the impact of the data set size on NPOs?

Several researchers indicated the size of the NPO data set as a crucial problem for addressing NPOs as a separate group during the technology development process. Such a small data set could further corrode the quality of the data for the NPO sector. This is particularly problematic in terms of machine learning training.

One researcher concluded it is probably impossible to make an accurate machine learning model for NPOs as there are not enough NPOs inside each institution to make a robust model. It would likely be too costly. Likewise, as described in Section II, Theme 1 - Effectiveness & Reliability, there are no feasible data sharing options across institutions to overcome the data set quality issues.

Even if developers created an NPO-specific algorithm, it would be riddled with issues due to the small size of the data sets. In cases where there is too little data for too many features in the model, the model may see patterns that do not exist and become biased by outliers, resulting in the overfitting issues we described in Section II, Theme 1 - Effectiveness & Reliability.

> If the development of NPO-specific technology is not realistic due to data set limitations, and if there are no financial incentives for businesses to calibrate their technology with the profile of NPO clients in mind, the question remains – how will NPO-specific issues be addressed through the design, development and deployment of emerging technologies for AML/CFT? How can we ensure the use of this technology will not disproportionately affect NPOs?

Is there room for communication or inclusion of NPOs in the design and development of emerging technologies?

In all interviews, respondents stated that NPOs as (potential) customers are generally not included in the process of either discussing or developing the technology models for AML/CFT compliance. No external stakeholders from the NPO sector (or the human rights or data ethics communities, for that matter) seem to be included in the development project teams.[69] At most, internal legal departments or personnel are included in the process.

The lack of NPO participation means potential negative impacts or biases against NPOs will likely remain unnoticed. This was confirmed by all interviewees, as they could not share any insight or data about their technology's impact on NPOs. However, one

69 It is, however, worth noting that one participant posited that although financial institutions do not include external experts, their hiring practices suggest some openness to engaging with alternative points of view. There appear to be efforts to bring data ethicists and human rights experts in-house, although it is not clear how consequential those efforts will be in the long-term.

FinTech company showed interest in collaborating with NPOs on use cases for their tech development.

> With no specific attention provided to the issues and challenges of the NPO sector, the technology development might likely mirror and embed existing negative impacts. It is problematic that FinTech businesses and financial institutions do not know, understand or consider NPO sector challenges during the technology development. NPOs should be able to understand why algorithms are flagging their behaviour as suspicious, as it often correlates to behaviour that is dissimilar from business clients' but nevertheless benign. However, if NPOs ask for this information directly, that in itself might be considered suspicious.
>
> On the other hand, different NPOs work on cultivating a greater understanding and knowledge about their work, addressing financial institutions and regulators. Open communication and learning is the best pathway to address some of the inclusion issues faced by NPOs.

Does emerging technology show any promise for solving the problems of NPOs?

Some FinTech companies believe their technology could aid in lowering the "false positive" matching of customers, including NPOs, indirectly assisting in addressing some of the issues of false suspicious flags or discrimination. However, their tools currently do not go far enough. Suppose a client segment was consistently rated as higher risk (consciously or unconsciously). The model could pick up on the trends and quantitative metrics (e.g. "you have many clients in this segment you are highlighting as high-risk") but not necessarily identify why the trend is there.

One financial institution mentioned that, in its view, machine learning is not a holy grail for compliance effectiveness, and the rule-based approach will likely remain the norm in the next ten years. In its view, machine learning could, however, improve the effectiveness and efficiency of the processes. In addition, the technology itself should not negatively impact NPOs, as there is always human oversight. Nevertheless, to have a beneficial impact on NPOs, this should be accompanied by strict governance and mature processes.

One FinTech company noted that, if one of their financial institution clients detected systematic de-risking of NPOs and wanted to address this issue, it could either partially adapt the results of the system or require more in-depth assistance from them to reconfigure the system, for instance, changing the risk scoring. We could not confirm whether such situations have, in fact, occurred.

The extent to which emerging technology can effectively improve the financial inclusion of NPOs remains unclear. FinTech may increase customer ability to initially access services or increase the understanding of rules and regulations; however, it is still unknown how it may help mitigate the existing de-risking issues. In addition, it is not clear whether machine learning could ensure fewer false positives over time, specifically in the NPO sector. It also seems that the problem-solving responsibility might be systematically "handed over" from developers to their clients and back, leaving the issues unresolved due to a general lack of agency and accountability.

Emerging technology can, in theory, make data sharing easier and safer, meaning KYC and CDD could become faster and more accurate. The focus might eventually shift from traditional rule-based, "know your client" approaches to risk-based, "know your data" approaches. This development could reduce the perceived risk of NPOs, focusing more on anomalies in the data patterns. However, there are currently not enough statistics or data to confirm this potential benefit.

Table 7. Recommendations to Improve Impact on NPOs		For
7.1.	The FATF should encourage more research on the impact of emerging forms of technology on marginalised and under-served communities, including the NPO sector.	FATF
7.2	The FATF should facilitate multistakeholder and cross-sector collaboration between technology creators and operators, FinTech businesses, financial institutions, regulators, governments and representative groups of financial services users, including the NPO sector. A collaborative model that breaks apart the silos that typically exist in technology discussions should be actively promoted.	FATF FIs FinTechs Regulators Governments NPO sector
7.3	During the design, development and deployment of their technology, technology creators should engage experts from a wide set of backgrounds, including human rights, NPOs and data ethics. They should assemble teams that include problem-solvers as well as problem-finders. We cannot fix technology or the problems it causes unless those problems are exposed first. This entails considering unintended consequences on multiple levels, surfaced through multiple perspectives.	FinTechs FIs

7.4	Financial institutions should measure the impact of their compliance technology on different types of customers in order to detect and mitigate individual and societal harm.	FIs
7.5	NPOs should be afforded more information, proper communication channels and increased collaboration with financial service providers to expose and improve the issues they face.	FIs

Conclusion

This report has provided an initial mapping of the emerging technologies deployed for financial compliance in order to better understand how emerging technologies for AML/CFT are impacting the NPO sector. In this conclusion, we set out the main findings of our research, discuss its limitations, and provide final recommendations that can be adopted by multiple actors working within the field of AML/CTF compliance.

Main findings

Three sub-questions were formulated to assess the impact of emerging technology deployed in AML/CTF compliance on NPOs: (i) the nature and type of emerging technologies used in this setting, (ii) the standards for design, development, deployment and operation of emerging tech compliance solutions, and (iii) the overall impact on the NPO sector. The main findings emerging from our research on those three fronts are as follows.

Nature and type of emerging technologies used for AML/CFT

1. FinTech businesses, financial institutions, regulators, and supervisors use different emerging technologies to improve compliance practices.
2. Opinions about the usefulness of these technologies and their potential to replace the rule-based approach that has been dominant in compliance practices for the past decades are divided.
3. Most of the conditions for the design, development and deployment of new technologies remain somewhat experimental. Clear guidelines, benchmarks and impact assessments are needed. Development pipelines include robust legal and regulatory compliance controls but no specific impact assessment or review.

Product design, development, deployment and operation

4. Although certain technologies - such as AI - are touted as superior to humans in their ability to assess probabilities and deal with complexity, claims about the benefits harnessed by technology were hard to verify due to a lack of adequate metrics to measure the effectiveness and reliability of these tools.
5. Concerns over the state of advancement and effectiveness of these technologies still exist. Many participants criticised the bluntness of some of these tools and highlighted issues with data quality and data sharing yet to be solved.

6. Compliance teams prioritise accuracy and efficiency above outcomes such as fairness and financial inclusion. Developers and operators focus heavily on risks related to the functioning of their systems (how they are built, how predictably they operate) but not so much on the systems' broader structural and societal impact.

7. Businesses developing or using FinTech made scant disclosures about errors and did not always appear to have considered unintended consequences or reflected on the wider socio-economic impact of their technology.

8. Stated commitments to promote fairness or avoid discriminatory effects are rarely accompanied by concrete measures to foster those values. Many FinTech businesses do not consider fairness and discrimination issues mission-critical at the outset of their journey. These concerns are typically deferred until they are more mature or, alternatively, shifted to end-users and customers.

9. Cybersecurity and privacy concerns seem to be taken rather seriously - even by start-ups - due to strict legal requirements such as the GDPR. However, the observed business practices are unlikely to afford data subjects genuine agency over their data and the inferences that can be extracted from it.

10. Businesses seem to focus predominantly on ensuring automated decisions are explainable to operators, regulators and supervisors. Not much heed is paid to explaining the rationale behind decisions to the subjects ultimately affected by those decisions. A need for secrecy is frequently depicted as a necessary precaution against strategic classification and other risks, foreclosing any possibility of analysing and improving potentially flawed models.

11. Despite assertions that human control over the technology is critical, neither developers nor deployers of compliance technology painted a thorough picture of the conditions surrounding human control over algorithmic-generated decisions. Technology developers and procurers do not set minimum technological literacy and competence standards or guidance for the technology operators. The data we gathered is indicative of human involvement but not necessarily of human control.

12. In most cases, there is no concrete framework laying out who is responsible for what action, who has recourse to which corrective actions and what information will be disclosed to enable problem-solving procedures.

13. There do not seem to be clear avenues for allocating responsibility between the agents involved in creating and operating a system.

14. Our research did not uncover any concrete procedures for contesting these decisions. Even when a technologically-enabled decision substantially impacts a person or group, the channels for challenging it are not readily apparent or feasible.

Impact on the NPO sector

15. Representatives from the NPO, human rights or data ethics sectors are seldom included in the teams responsible for designing and developing the technology behind financial compliance solutions.
16. Most FinTech businesses do not have actionable insights about NPOs. Many lack information about the needs and operation of NPOs and how their products impact NPOs.
17. The lack of NPO-specific knowledge or participation suggests that potential negative impacts or biases against NPOs will likely remain unnoticed.
18. NPOs are often globally treated as high-risk customers due to generally misguided understandings of AML/CFT requirements. The possibility that this flawed approach will permeate the design and development of new technologies is especially concerning given the difficulties in challenging some of these decisions.
19. Technology solutions are not properly calibrated for NPOs, whose profile and behaviour are different from the business customers that financial institutions predominantly target and serve. Given the small data set size for NPOs, models could very likely be overfitted and spurious correlations and other misguided inferences could be drawn.
20. As they represent such a small group outside the set target demographic for most businesses, NPOs are unlikely to become a specific customer segment with a bespoke set of rules and procedures addressing their systemic issues. Even if emerging technologies could provide such solutions, incentives are not aligned for businesses to allocate their resources to designing technology with the NPO sector in mind.

In summary, new technologies have changed and will continue to change the compliance landscape in upcoming years. They have pushed the emergence of different FinTech companies and altered practices within financial institutions. Our research revealed that all respondents are committed to tackling financial crime and believe that new technologies have the potential to improve AML/CFT processes.

In our view, however, that potential will only be realised if technology development and use are based on a solid understanding of (i) their strengths and vulnerabilities, (ii) the skill sets and conditions required for their effective operation, (iii) the proper remedies for challenging and assigning responsibility for their outcomes. We should not risk uninformed technology adoption in the financial sector, a fundamental component of the social order.

At a minimum, we hoped to confirm that the developers and adopters of these technologies have considered the questions explored in this report - particularly the ones included in each of the themes covered in Section II of the report - not only from the point of view of ordinary business clients but also from the perspective of nonprofit organisations. That would be a satisfactory basis for maintaining informed trust in

the overall system. However, our findings do not provide a solid enough foundation for nonprofits to trust that their needs are being taken into account by those developing and adopting these technologies.

Limitations

This study has some limitations, chief among them the size and diversity of its research sample. Considering the breadth of institutions we reached out to at the outset of this project, the limited number of secured interviews seems to reflect a general lack of interest from the FinTech sector in engaging with the NPO sector on this subject. A more authoritative entity in the field or the support of a convener is likely required to drive interest in this type of study.

Furthermore, the businesses that were receptive to this project were predominantly FinTech start-ups and scale-ups. The insights kindly shared with us by representatives of these businesses are unlikely to be representative of medium-sized or multinational enterprises. Although caution against extrapolation is warranted, it was still valuable to establish our research participants' status and stance on these topics, as they will be indicative of what smaller organisations with limited resources are considering and doing. These are valuable data points for further action and policy-making.

Nevertheless, there is a great deal we were not able to confirm. Sometimes, the research participants did not have specific data relevant to NPOs. Other times, they did not feel it was prudent to share that information with us or the wider public, even in anonymised format.

As mentioned elsewhere in this report, without a baseline level of transparency toward a wide range of stakeholders (including non-experts and the general public, at times), there is no way to trust or verify that a given decision that has been aided or mediated by emerging technology can be explained or, if necessary, corrected. There is no basis to confirm that these applications adhere to normative or legal standards and produce fair results. There are no means to ensure that those engaged in the design, development, deployment, operation and validation of the effectiveness of these applications can be held accountable for negative outcomes.

Final recommendations

Many of the issues identified in this report have the potential to coalesce into a sprawling sector-wide crisis in the field of compliance. This is a field with so many players and moving pieces that simple, one-size-fits-all solutions are likely not feasible. As such, in addition to the recommendations presented in Tables 1-7 of this report, we leave each of the main groups of stakeholders in the arena with a final set of broad recommendations and food for thought in the hope that this helps move the ecosystem forward for all.

Table 8. Final Recommendations

	For standard-setters, policymakers and regulators
1	Take a more active role in assessing the impact of these technologies, considering unintended consequences for groups such as NPOs. Factor those consequences in the cost-benefit analysis that determines the overall effectiveness of these emerging technologies. Set minimum standards for the development and operation of these technologies.
2	Use your standard-setting powers to act as a convener of multistakeholder forums combining industry, academia, NGOs and NPOs, government, regulators and supervisors. Pulling together the input from all the relevant stakeholders will almost certainly require some institutional initiative. Make NPOs a part of those critical conversations, both as an affected group and as representatives of other affected groups. Consolidate the result of those discussions and deliberations into international norms and standards.
3	Increase funding for multidisciplinary research and education on the ethics, safety, privacy, fairness, trustworthiness and overall impact of emerging technologies used for AML/CFT on human rights and societal outcomes. The impact of technology should be addressed not only at the academic and civil society level but also near businesses, government and policymakers.

	For technology developers and deployers
1	Reflect on and operationalise the principles discussed in each of the themes included in Section II of this report. Consider the societal outcomes of your technology, its unintended consequences and your overall impact on broader issues like the financial exclusion of communities and groups such as NPOs. Determine the ways your technology can and cannot improve those issues.
2	Create a human rights impact framework tailored to your business that articulates your key ethical standards, identifies relevant external and internal stakeholders, and implements a robust governance structure. In addition, draw inspiration from the recommendations included in Tables 1-7 report to optimise guidance and tools for your workforce. While the impact framework will provide high-level guidance, more granular guidance at the product level is helpful for your operations. Build organisational awareness around this framework. Foster a culture where these issues are discussed at critical junctures, and a setup where employees can raise their concerns to a specific individual or body.
3	Externally, engage other stakeholders to learn from them as knowledge partners. Recognise that your products may be ethically developed but unethically deployed, and it is important to engage external stakeholders to determine how your product has affected them. Identify key stakeholders early in the development process and include them in the design, development and post-deployment monitoring stages. Participate in multistakeholder forums and policy design workshops.

	For financial crime practitioners, researchers and civil society
1	Collaborate to provide actionable tools that early-stage FinTech ventures are unlikely to have the resources to develop themselves. For example, a FinTech AML/CFT Playbook (including a list of core values and principles, typologies of harm and mitigating measures that could improve the harms and risks stemming from irresponsible tech development)[70] could help businesses better balance the demands for economic growth, financial crime reduction and the mitigation of risks raised by technology.
2	Research and investigate the real costs and benefits of using emerging technology in compliance and of AML/CFT measures in general. Interesting research pathways include empirical studies of the ways in which banks may actually profit from failing to comply with AML regulations[71] and into the compatibility of AML regulations with fundamental rights[72] and regulations[73].
3	Reflect on the essential questions emerging from that research. If FinTech for compliance purposes cannot prove its own effectiveness (due to a lack of valid, actionable metrics) and if it is disproportionately impacting certain groups that it is not calibrated for, should its development and deployment remain unhindered? Or should it be subject to more rigorous control, perhaps starting with limited use in a controlled test environment - similar, for instance, to the requirements for pharmacological development? Likewise, if AML/CFT regulations themselves are inherently discriminatory and not even necessarily effective in stopping money laundering or terrorism financing, should their proportionality and legitimacy be placed under the spotlight, tested, perhaps even litigated? Until and unless we have answers for some of these pressing questions, should Recommendation 8[74] stand?

70 The IEEE, "Ethically Aligned Design", p. 245.

71 See Ferwerda, Joras and Thimo Zwiers, "Do Banks Profit from Failing to Control Money Laundering? An Empirical Study." Working Paper for Third International Research Conference on Empirical Approaches to AntiMoney Laundering and Financial Crimes. Bahamas 2022. Available at https://aml-cft.centralbankbahamas.com/assets/images/pdf/conferences/2022/14_ferwerda_and_zwiers_2022_bank_fines_final_version_submitted_for_bahama_conference.pdf (Accessed 25 May 2022).

72 See for instance Sciurba, Michele "The Incompatibility of Global Anti-Money Laundering Regimes with Human and Civil Rights – Reform Needed?"' (Baden-Baden: Nomos, 2019); Bertrand, Astrid, Winston Maxwell, and Xavier Vamparys, "Do AI-based anti-money laundering (AML) systems violate European fundamental rights?" International Data Privacy Law (2021).

73 See for instance Maxwell, Winston, "The GDPR and private sector measures to detect criminal activity." Revue des Affaires Européennes-Law and European Affairs (2021).

74 FATF, "Best practices. Combating the abuse of non-profit organisations (recommendation 8)" Paris: FATF, 2015. Available at https://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf. (Accessed 27 May 2022).

Comprehensive coverage of all the issues within our scope is not feasible in a single report. Therefore, we will expand this initial mapping exercise with reflections and experiences of NPOs and banking regulators and explore recent efforts by multilateral institutions such as the United Nations to use similar technologies for security and counter-terrorism purposes.

Appendixes

A. Research participants

The table below presents an overview of the role and affiliation of the main research participants, duly anonymised to ensure the participants cannot be identified in accordance with the study's data management policies.

	Source	Organisation	Size	Maturity	Main Region	Role
1	Interview	Financial Institution	Large (251+ Employees)	10+ Years	Western Europe	Head of Innovation; Human Rights Advisor
2	Interview	Financial Institution	Large (251+ Employees)	10+ Years	Western Europe	Head of Client Activity Monitoring
3	Interview	Financial Institution	Medium (51-250 Employees)	3-5 Years	North-eastern Europe	Partner and Advisor
4	Interview	FinTech Firm	Large (251+ Employees)	5-9 Years	USA	Director (Technology)
5	Interview	FinTech Firm	Medium (51-250 Employees)	5-9 Years	Western Europe	Business Development
6	Interview	FinTech Firm	Small (0-50 Employees)	3-5 Years	Central Europe	Head of Public Sector; Product Manager
7	Interview	FinTech Firm	Small (0-50 Employees)	5-9 Years	Middle East	Founder and President; VP of Marketing

8	Interview	FinTech Firm	Small (0-50 Employees)	0-3 Years	Western Europe	Head of Compliance
9	Interview	FinTech Firm	Small (0-50 Employees)	3-5 Years	Eastern Europe	CEO and Product Developer
10	Interview	FinTech Firm	Small (0-50 Employees)	5-9 Years	North-western Europe	CEO and Founder
11	Conference	FinTech Firm	Large (251+ Employees)	10+ Years	Central Europe	CEO
12	Conference	FinTech Firm	Small (0-50 Employees)	3-5 Years	North-western Europe	Vice President
13	Interview	Supervisor	N/A	N/A	Western Europe	Data analyst
14	Interview	Financial Advisory Firm	Large (251+ Employees)	N/A	Western Europe	Senior Consultant
15	Interview	Research Institute/ University	N/A	N/A	Western Europe	Director of Law and Technology; PhD Students
16	Interview	Research Institute/ University	N/A	N/A	Western Europe	Assistant Professor of Informatics
17	Interview	Research Institute/ Think Tank	Large (251+ Employees)	N/A	North-western Europe	Research Fellow
18	Conference	Research Institute/ University	N/A	N/A	USA	Professor of Finance

19	Conference	Panel inc. Financial Institutions, Financial Services Companies, Universities	N/A	N/A	N/A	Principal, Digital Assets Risk & Compliance; Snr Lecturer in Financial Technology; Snr Manager Sanctions Policy & Complex Advisory
20	Conference	Panel inc. Financial Institutions and Law Enforcement	N/A	N/A	N/A	Fraud and AML Devel-opment Officer; Financial Crime Compliance Lead; Head of Compliance
21	Conference	Panel inc. FinTech Firms, Payment Providers, Universities, Financial Institutions	N/A	N/A	N/A	Director of Product Strategy; Professor of Cyber Systems Engineering; Director of Global Product Sales; Head of Innovation & Design
22	Conference	Panel inc. Financial Institutions and FinTech Firms	N/A	N/A	N/A	Head of Financial Crime; Head of Compliance and AML and others

23	Conference	Panel inc. Law Enforcement, FinTech Firms, Financial Institu-tions and Insurance Companies	N/A	N/A	N/A	Detective Sergeant; Solutions Director; Financial Crime Intelligence and Investigations Director and others

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

www.ecnl.org
@enablingNGOlaw