Rita R. Soares, Consultant - Tech and Human Rights

Presentation for ECNL | Haarlem, June 27, 2023

Fintech Findings 101

Lessons from research on emerging technologies used for AML/CFT and their impact on the NPO sector

INTRODUCTIONS

TABLE OF CONTENTS

01

THE LANDSCAPE

What we knew
and what we didn’t

02

THE PROJECT

What we set out
to find out

03

THE PROCESS

Initial plans and
adjustments

04

THE FINDINGS

What we learned

05

THE LIMITATIONS

What we couldn’t

06

THE WAY FORWARD

What you can do

01

THE LANDSCAPE

What we knew and
what we didn't

Known: Financial and regulatory tech growth

1. In July 2021 the FATF published a report indicating ET could be used to make AML/CFT measures "faster, cheaper and more effective"
2. The financial sector seemed to be widely deploying big data analytics, machine learning and blockchain to reduce cost and time spent conducting due diligence and transaction monitoring
3. Fintech focused on compliance, such as RegTech and SupTech, was growing exponentially, with the global market for regulatory technology expected to be worth $33.1 billion by 2026
4. Main drivers for growth:
   a. Dire compliance statistics
   b. Belief that tech solutions can help improve those statistics
   c. Belief that tech solutions can ultimately improve financial inclusion

Known: Challenges faced by NPOs

1. NPOS (and humanitarian relief organisations in particular) have fallen victim to the financial industry's tendency to de-risk in order to avoid penalties arising from regulatory noncompliance,
2. This results in financial exclusion: difficulties opening bank accounts, delayed transactions, unexplained account closures
3. Experts and international organisations such as the FATF and IMF posit that emerging tech-powered compliance solutions may reduce these obstacles… but do they?

Unknown: Impact of ETs on NPOs challenges

1. The July 2021 FATF report acknowledged the importance of mapping risks and unintended consequences of emerging tech across the spectrum of financial services users - didn’t address current or best practices
2. Unclear how these technologies are developed and tested by Fintechs, how financial institutions procure, deploy and operate these technologies, or what safeguards are installed to mitigate unintended consequences
3. Unclear whether new Fintech solutions are maintaining or exacerbating trends to de-risk NPOs
4. Unclear whether they are ultimately widening or shrinking civic space and affecting human rights
5. More in-depth research into the effects of ETs on the issues of de-risking and financial exclusion faced by NPOs needed.

02 THE PROJECT

What we set out
to find out

Research objectives

1. Gain better understanding of the effects of the use of ETs for AML/CFT on the nonprofit sector
2. Determine whether the increased reliance on Fintech for compliance purposes is maintaining or exacerbating the trend to de-risk or, alternatively, enabling a more inclusive access to financial services that could benefit traditionally underserved demographics such as NPOs
3. Approach FIs, Fintech companies, supervisors and other experts to understand what these technologies entail, and how they are developed and deployed in the financial industry
4. Ultimately assess that impact on NPOs and provide recommendations
5. Move beyond binary tech-optimistic or tech-pessimistic perspectives

Operating principles

1. Public confidence in the technology used in the financial sector is critical to a well-functioning society.
2. A lack of confidence in these technologies could result in a loss of confidence in the financial system as a whole.
3. Trust and confidence should be sought not only from those engaged in designing or deploying technology but also from those expected to use it and who are affected by it.
4. 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.

But how do we find this information?

03

THE PROCESS

Initial plans and adjustments

Areas of inquiry

1. What kind of ETs are used for AML/CFT?
2. How is this tech designed, developed, deployed and operated?

   Post-facto review of the findings through the lens of six key areas of analysis linked to responsible tech development:

   (1) Effectiveness & Reliability,
   (2) Fairness & Discrimination,
   (3) Security & Data Privacy,
   (4) Transparency & Explainability,
   (5) Human Oversight & Technical Competence,
   (6) Accountability & Contestability.

3. Is this technology maintaining, exacerbating or mitigating issues for NPOs?

Paths of inquiry

1. Interviews
   a. Created Questionnaire (loosely based on Annex B of the July 2021 FATF Report) as a guide for semi-structured interviews to take place alongside conference attendance and desk-based research
   b. Compiled list of target experts from the Fintech and FI sectors
   c. Reached out through existing networks (LinkedIn), recommendations (snowballing) and cold-calling/emailing contact addresses and pages
   d. Due to low success rates from the outreach into the banking and Fintech sectors and suboptimal sample size, the initial scope of research was expanded to think tanks and consultancies
   e. Interviewed and consulted 20+ experts from financial institutions, Fintech firms, supervisors, think tanks, research centres, policy institutes, financial services consultancy firms and law enforcement.

Paths of inquiry (cont.)

1. Conference attendance
   a. Attended virtual conferences where we engaged with some of the conference speakers and tested product demos

2. Desk-based research
   a. Conducted a desk-based review of governmental and non-governmental policies and reports, media reports and grey literature

3. Research method and data analysis
   a. Qualitative data reviewed to identify themes and emerging patterns
   b. Thematic analysis and coding of interview transcripts, reports and field notes - inductive code framing table
   c. Analysis presented in Q&A format to improve readability (but the format is different from the original Questionnaire)

04

THE FINDINGS

What we learned

FINDINGS – THREE INQUIRY AREAS

I.

Emerging technologies used for AML/CFT purposes

II.

Standards for technology design, development, deployment and operation

III.

Impact on the NPO sector

I. Emerging technologies used for AML/CFT purposes

1. Fintech businesses, financial institutions, regulators, and supervisors use different ETs to improve compliance practices.
2. Research participants relied on supervised and unsupervised ML, NLP, OCR, APIs, Fuzzy Logic, Phonetics, Computational Linguistics, Cryptography and big data analytics techniques to provide tech solutions for several AML/CFT Processes
   a. Helpful Tech Primer for AML/CFT here
   b. Examples of the impact of this tech in the compliance landscape

I. Emerging technologies used for AML/CFT purposes (cont.)

1. FATF's thesis: better ways to interpret data, and share it with stakeholders, could benefit compliance and promote risk-based approaches
   a. Do ETs for AML/CFT actually deliver on this?
   b. 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.
2. FATF's proviso: ETs 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
   a. Is this being achieved?
   b. If so, at what cost?

FINDINGS – THREE INQUIRY AREAS

I.

Emerging technologies used for AML/CFT purposes

II.

Standards for technology design, development, deployment and operation

III.

Impact on the NPO sector

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

1. Questions:
   a. What are they key benefits and risks of relying on ET for compliance purposes?
   b. Are those risks known by those developing and operating such technology?
   c. Are there safeguards or risk mitigation measures in place?
2. Teaser: 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. There are significant causes for concern.

QUESTION BRAINSTORM

(1) Effectiveness & Reliability,

(2) Fairness & Discrimination,

(3) Security & Data Privacy,

(4) Transparency & Explainability,

(5) Human Oversight & Technical Competence,

(6) Accountability & Contestability.

II. Standards (cont.)
1. Effectiveness & Reliability

1. Questions:
   a. Are ET systems operating in a reliable manner, consistent with their intended purpose and without unforeseen or unintended consequences?
   b. Can the developers and operators of ET demonstrably prove and measure the effectiveness and fitness for purpose of their technology through valid, credible and actionable benchmarks or metrics?
   c. If such effectiveness metrics do exist, who has access to them?

2. Teasers:
   a. 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.
   b. Concerns over the state of advancement and effectiveness of these ETs 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.
   c. Scarce disclosure of of errors/inaccuracies or unintended consequences.

II. Standards (cont.)
2. Fairness & Discrimination

1. Questions:
   a. Is the technology accessible, inclusive and free from bias?
   b. Does the technology directly or indirectly result in unfair discrimination against any individuals, groups or communities?
   c. Is the technology designed and operated to ensure fairness and financial inclusion?

2. Teasers:
   a. 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.
   b. Businesses did not always appear to have considered unintended consequences or reflected on the wider socioeconomic impact of their technology.
   c. 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 these issues mission-critical at the outset of their journey. Either deferred until they are more mature or shifted to end-users and customers.

II. Standards (cont.)
3. Security & Data Protection

1. Questions:
   a. Do the emerging tech systems respect and protect the data subjects' privacy and ensure their data security?
   b. 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?

2. Teasers:
   a. Cybersecurity and privacy concerns seem to be taken rather seriously (even by start-ups and scale-ups) due to strict legal requirements such as the GDPR.
   b. 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.
   c. Data subjects receive little more than the opportunity to review predefined terms and conditions and privacy policies designed to protect institutional interests - concerning when the value that can be extracted from data is so hard to predict.
   d. Some FIs mentioned that any customer who sought to learn more could be flagged for suspicious behaviour.

II. Standards (cont.)

4. Transparency & Explainability

1. Questions:
   a. Is there sufficient disclosure and transparency regarding the use of ET, such that impacted individuals can understand when and how they are affected by it?
   b. Are the basis of decisions traceable, understandable and explainable from the perspective of (i) those developing the technology, (ii) those operating it, and (iii) those affected by it?

2. Teasers:
   a. Transparency and explainability are mostly focused on operators, regulators, and supervisors, with little attention to the individuals affected by the decisions.
   b. 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.
   c. 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.

II. Standards (cont.)

5. Human Oversight & Technical Competence

1. Questions:
   a. Is the technology subject to human oversight and control?
   b. 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?
   c. Do developers specify the knowledge and expertise necessary for their systems' safe and successful operation, and are those requirements adhered to by operators?

2. Teasers:
   a. The overwhelming response was that human oversight existed at all critical stages of the process, with human control over the final decisions.
   b. Human oversight is present, but the level of control and technical competence varies.
   c. Neither developers nor technology deployers painted a thorough picture of the conditions surrounding human control over algorithmic-generated decisions.
   d. 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.

II. Standards (cont.)
6. Accountability & Contestability

1. Questions:
   a. 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?
   b. 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?
   c. 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?
2. Teasers:
   a. 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.
   b. There do not seem to be clear avenues for allocating responsibility between the agents involved in creating and operating a system.
   c. We did not uncover concrete procedures for contesting these decisions.

FINDINGS – THREE INQUIRY AREAS

I.

Emerging technologies used for AML/CFT purposes

II.

Standards for technology design, development, deployment and operation

III.

Impact on the NPO sector

III. Impact on the NPO sector

1. Questions:
   a. Are NPOs treated as a specific customer segment?
   b. What is the impact of the data set size on NPOs?
   c. Is there room for communication or inclusion of NPOs in the design and development of ETs?
   d. Does ET show any promise for solving the problems of NPOs?

2. Teaser:
   a. We know the financial sector's approach to nonprofits is inconsistent, often treating them as high-risk customers without considering their unique needs and operations.
   b. Fintech businesses lack NPO-specific knowledge, suggesting that technology solutions are not adequately tailored to the sector.

III. Impact on the NPO sector (cont.)

1. Representatives from the NPO, human rights or data ethics sectors are seldom included in the teams responsible for designing and developing tech for financial compliance solutions.
2. Most businesses do not have actionable insights about NPOs and lack information about the needs and operation of NPOs and how their products impact NPOs.
3. The lack of NPO-specific knowledge or participation suggests that potential negative impacts or biases against NPOs will likely remain unnoticed.
4. 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.
5. 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.
6. As they represent such a small group outside the target 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 ETs could provide such solutions, incentives are not aligned for businesses to allocate their resources to designing technology with the NPO sector in mind.

DISCUSSION

If the development of NPO-specific tech is not realistic due to data set size & sharing limitations, and if there are no incentives for businesses to calibrate their tech with the profile of NPO clients in mind...

1) how can NPO-specific issues be addressed through the design, development and deployment of ETs for AML/CFT?
2) How can we keep this technology from disproportionately affecting NPOs?

05 THE LIMITATIONS

What we couldn’t confirm

Limitations

1. The limited number of secured interviews suggests a general lack of interest from the Fintech sector in engaging with the NPO sector on this subject
2. The research participants were mainly Fintech start-ups and scale-ups, which may not be representative of medium-sized or multinational enterprises.
3. There were instances when the research participants did not have specific data relevant to NPOs, or they did not feel comfortable sharing that information, even in an anonymized format.
4. Further research is needed to examine how larger financial institutions and actors in different jurisdictions make use of these technologies and how NPOs and their needs can be better integrated into the design, development and deployment of these technologies.

06 THE WAY FORWARD

What you can do

Next steps

1. If you're carrying on with similar research, some tips:
    a. Read our report and recommendations (not in this presentation)
    b. Create a short note on the project’s background and a very short list of topics you would like to discuss (the full research questionnaire would be overwhelming
    c. Don't approach anyone between Thanksgiving and end of January
    d. Really, no one will reply. Wait until February

2. Use this presentation to assemble your research toolkit:
    a. Research questionnaire
    b. Outreach targets list
    c. Data analysis framework
    d. Questions (Q&A format) for framing and analysing the findings

APPENDIXES

RESEARCH QUESTIONNAIRE

INDUCTIVE CODE FRAME

OUTREACH TARGETS LIST

SURVEYED TECH PROCESSES

FINAL PARTICIPANT LIST

ILLUSTRATION OF AI IN AML/CFT

Next steps (cont.)

1. During interviews:
   a. Structure the interview as a conversation rather than a questionnaire. Break it down by “themes” rather than go through questions
   b. If tech discussions are getting too high-level, ask for examples or provide an example yourself and ask the interviewee to elaborate
   c. If respondents cannot talk about their work because of privacy issues, ask them to describe hypothetical cases. Have some prepared
   d. If they cannot go on the record, consider keeping it off the record (info may become public via another source and it still helps the analysis)
   e. If throughout the interview there are mentions of other people or businesses who may be relevant for the research, ask for intros
   f. At the end of the interview, ask if the interviewee wants to add things not discussed but potentially relevant, and ask them what they see as the most pressing issues.

QUESTIONS?

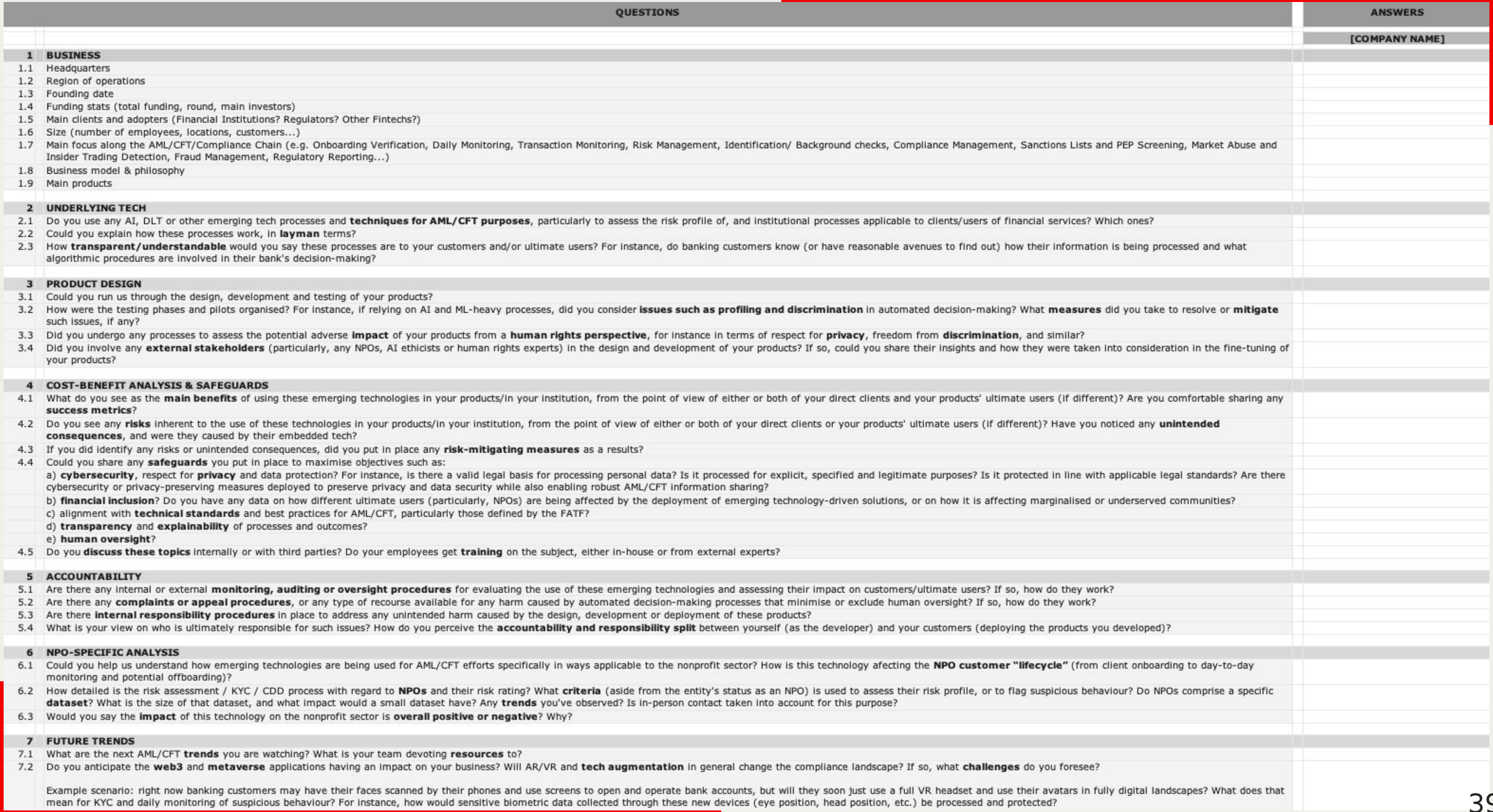
Thank you!

Feel free to connect in the future:

rita@rrsadvisory.com

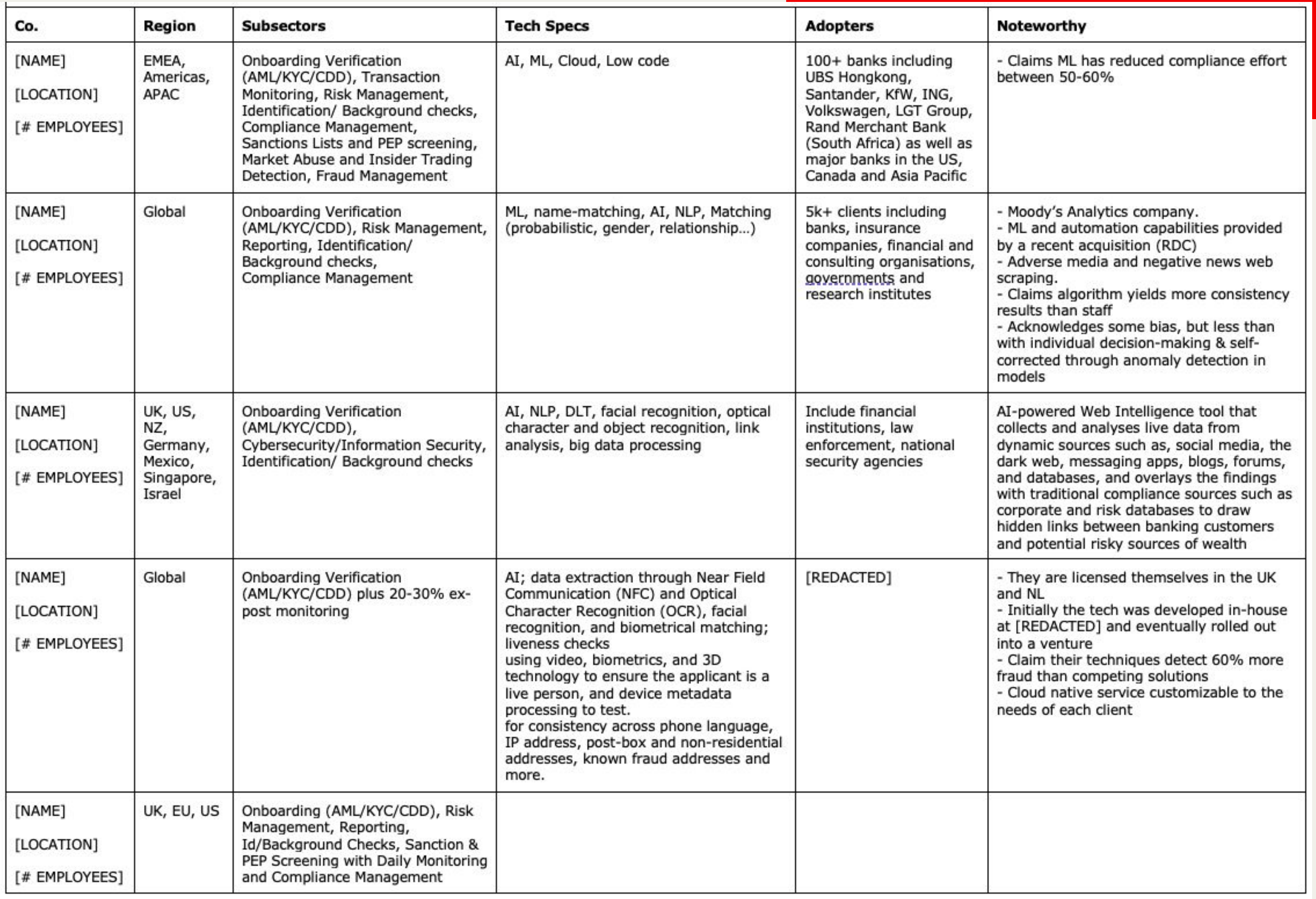
https://www.linkedin.com/in/rita-r-soares

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**



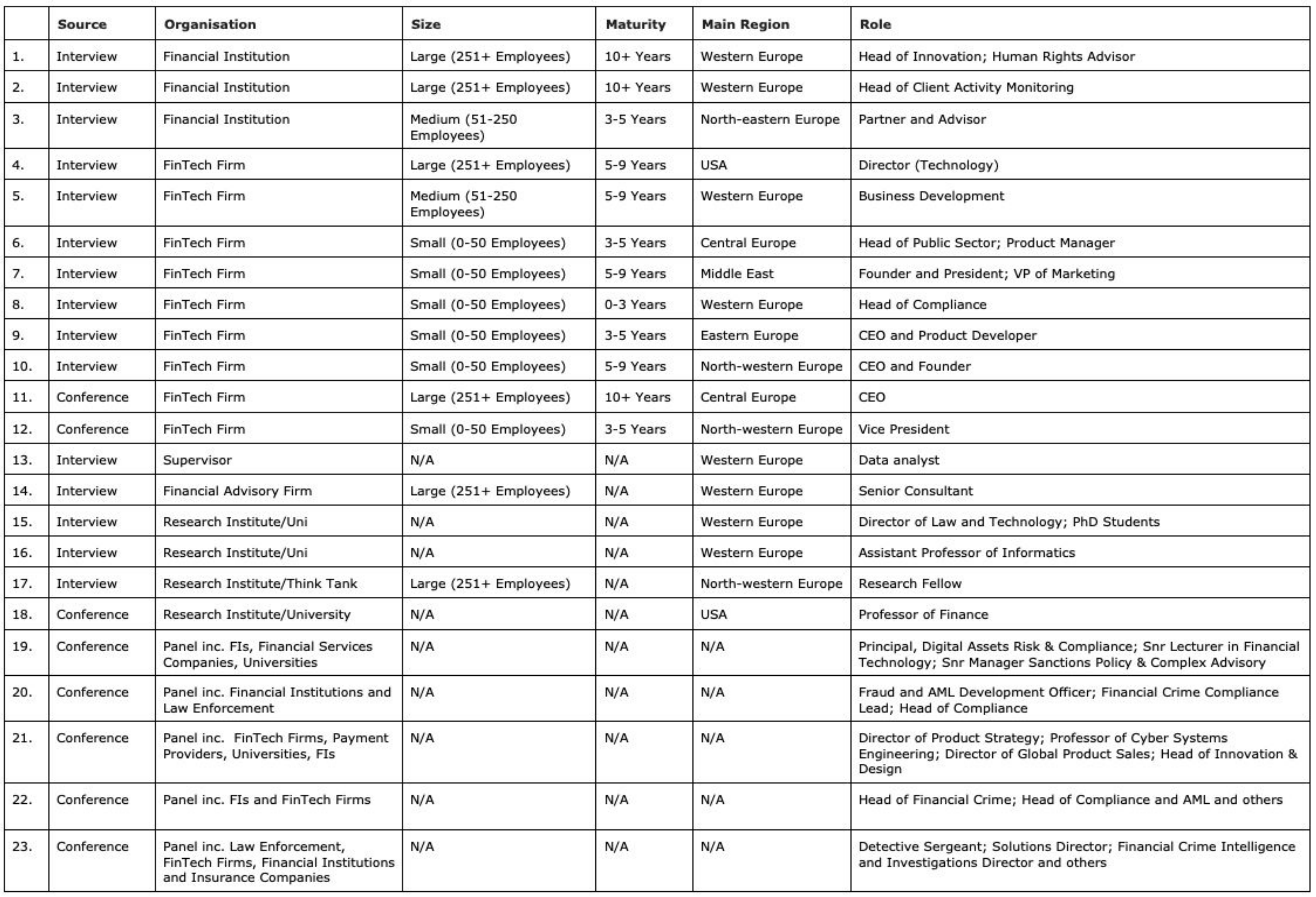
	QUESTIONS	ANSWERS
		[COMPANY NAME]
1	**BUSINESS**	
1.1	Headquarters	
1.2	Region of operations	
1.3	Founding date	
1.4	Funding stats (total funding, round, main investors)	
1.5	Main clients and adopters (Financial Institutions? Regulators? Other Fintechs?)	
1.6	Size (number of employees, locations, customers...)	
1.7	Main focus along the AML/CFT/Compliance Chain (e.g. Onboarding Verification, Daily Monitoring, Transaction Monitoring, Risk Management, Identification/ Background checks, Compliance Management, Sanctions Lists and PEP Screening, Market Abuse and Insider Trading Detection, Fraud Management, Regulatory Reporting...)	
1.8	Business model & philosophy	
1.9	Main products	
2	**UNDERLYING TECH**	
2.1	Do you use any AI, DLT or other emerging tech processes and **techniques for AML/CFT purposes**, particularly to assess the risk profile of, and institutional processes applicable to clients/users of financial services? Which ones?	
2.2	Could you explain how these processes work, in **layman** terms?	
2.3	How **transparent/understandable** would you say these processes are to your customers and/or ultimate users? For instance, do banking customers know (or have reasonable avenues to find out) how their information is being processed and what algorithmic procedures are involved in their bank's decision-making?	
3	**PRODUCT DESIGN**	
3.1	Could you run us through the design, development and testing of your products?	
3.2	How were the testing phases and pilots organised? For instance, if relying on AI and ML-heavy processes, did you consider **issues such as profiling and discrimination** in automated decision-making? What **measures** did you take to resolve or **mitigate** such issues, if any?	
3.3	Did you undergo any processes to assess the potential adverse **impact** of your products from a **human rights perspective**, for instance in terms of respect for **privacy**, freedom from **discrimination**, and similar?	
3.4	Did you involve any **external stakeholders** (particularly, any NPOs, AI ethicists or human rights experts) in the design and development of your products? If so, could you share their insights and how they were taken into consideration in the fine-tuning of your products?	
4	**COST-BENEFIT ANALYSIS & SAFEGUARDS**	
4.1	What do you see as the **main benefits** of using these emerging technologies in your products/in your institution, from the point of view of either or both of your direct clients and your products' ultimate users (if different)? Are you comfortable sharing any **success metrics**?	
4.2	Do you see any **risks** inherent to the use of these technologies in your products/in your institution, from the point of view of either or both of your direct clients or your products' ultimate users (if different)? Have you noticed any **unintended consequences**, and were they caused by their embedded tech?	
4.3	If you did identify any risks or unintended consequences, did you put in place any **risk-mitigating measures** as a results?	
4.4	Could you share any **safeguards** you put in place to maximise objectives such as:	
	a) **cybersecurity**, respect for **privacy** and data protection? For instance, is there a valid legal basis for processing personal data? Is it processed for explicit, specified and legitimate purposes? Is it protected in line with applicable legal standards? Are there cybersecurity or privacy-preserving measures deployed to preserve privacy and data security while also enabling robust AML/CFT information sharing?	
	b) **financial inclusion**? Do you have any data on how different ultimate users (particularly, NPOs) are being affected by the deployment of emerging technology-driven solutions, or on how it is affecting marginalised or underserved communities?	
	c) alignment with **technical standards** and best practices for AML/CFT, particularly those defined by the FATF?	
	d) **transparency** and **explainability** of processes and outcomes?	
	e) **human oversight**?	
4.5	Do you **discuss these topics** internally or with third parties? Do your employees get **training** on the subject, either in-house or from external experts?	
5	**ACCOUNTABILITY**	
5.1	Are there any internal or external **monitoring, auditing or oversight procedures** for evaluating the use of these emerging technologies and assessing their impact on customers/ultimate users? If so, how do they work?	
5.2	Are there any **complaints or appeal procedures**, or any type of recourse available for any harm caused by automated decision-making processes that minimise or exclude human oversight? If so, how do they work?	
5.3	Are there **internal responsibility procedures** in place to address any unintended harm caused by the design, development or deployment of these products?	
5.4	What is your view on who is ultimately responsible for such issues? How do you perceive the **accountability and responsibility split** between yourself (as the developer) and your customers (deploying the products you developed)?	
6	**NPO-SPECIFIC ANALYSIS**	
6.1	Could you help us understand how emerging technologies are being used for AML/CFT efforts specifically in ways applicable to the nonprofit sector? How is this technology afecting the **NPO customer "lifecycle"** (from client onboarding to day-to-day monitoring and potential offboarding)?	
6.2	How detailed is the risk assessment / KYC / CDD process with regard to **NPOs** and their risk rating? What **criteria** (aside from the entity's status as an NPO) is used to assess their risk profile, or to flag suspicious behaviour? Do NPOs comprise a specific **dataset**? What is the size of that dataset, and what impact would a small dataset have? Any **trends** you've observed? Is in-person contact taken into account for this purpose?	
6.3	Would you say the **impact** of this technology on the nonprofit sector is **overall positive or negative**? Why?	
7	**FUTURE TRENDS**	
7.1	What are the next AML/CFT **trends** you are watching? What is your team devoting **resources** to?	
7.2	Do you anticipate the **web3** and **metaverse** applications having an impact on your business? Will AR/VR and **tech augmentation** in general change the compliance landscape? If so, what **challenges** do you foresee? Example scenario: right now banking customers may have their faces scanned by their phones and use screens to open and operate bank accounts, but will they soon just use a full VR headset and use their avatars in fully digital landscapes? What does that mean for KYC and daily monitoring of suspicious behaviour? For instance, how would sensitive biometric data collected through these new devices (eye position, head position, etc.) be processed and protected?	

B



Co.	Region	Subsectors	Tech Specs	Adopters	Noteworthy
[NAME] [LOCATION] [# EMPLOYEES]	EMEA, Americas, APAC	Onboarding Verification (AML/KYC/CDD), Transaction Monitoring, Risk Management, Identification/ Background checks, Compliance Management, Sanctions Lists and PEP screening, Market Abuse and Insider Trading Detection, Fraud Management	AI, ML, Cloud, Low code	100+ banks including UBS Hongkong, Santander, KfW, ING, Volkswagen, LGT Group, Rand Merchant Bank (South Africa) as well as major banks in the US, Canada and Asia Pacific	- Claims ML has reduced compliance effort between 50-60%
[NAME] [LOCATION] [# EMPLOYEES]	Global	Onboarding Verification (AML/KYC/CDD), Risk Management, Reporting, Identification/ Background checks, Compliance Management	ML, name-matching, AI, NLP, Matching (probabilistic, gender, relationship…)	5k+ clients including banks, insurance companies, financial and consulting organisations, governments and research institutes	- Moody's Analytics company. - ML and automation capabilities provided by a recent acquisition (RDC) - Adverse media and negative news web scraping. - Claims algorithm yields more consistency results than staff - Acknowledges some bias, but less than with individual decision-making & self-corrected through anomaly detection in models
[NAME] [LOCATION] [# EMPLOYEES]	UK, US, NZ, Germany, Mexico, Singapore, Israel	Onboarding Verification (AML/KYC/CDD), Cybersecurity/Information Security, Identification/ Background checks	AI, NLP, DLT, facial recognition, optical character and object recognition, link analysis, big data processing	Include financial institutions, law enforcement, national security agencies	AI-powered Web Intelligence tool that collects and analyses live data from dynamic sources such as, social media, the dark web, messaging apps, blogs, forums, and databases, and overlays the findings with traditional compliance sources such as corporate and risk databases to draw hidden links between banking customers and potential risky sources of wealth
[NAME] [LOCATION] [# EMPLOYEES]	Global	Onboarding Verification (AML/KYC/CDD) plus 20-30% ex-post monitoring	AI; data extraction through Near Field Communication (NFC) and Optical Character Recognition (OCR), facial recognition, and biometrical matching; liveness checks using video, biometrics, and 3D technology to ensure the applicant is a live person, and device metadata processing to test. for consistency across phone language, IP address, post-box and non-residential addresses, known fraud addresses and more.	[REDACTED]	- They are licensed themselves in the UK and NL - Initially the tech was developed in-house at [REDACTED] and eventually rolled out into a venture - Claim their techniques detect 60% more fraud than competing solutions - Cloud native service customizable to the needs of each client
[NAME] [LOCATION] [# EMPLOYEES]	UK, EU, US	Onboarding (AML/KYC/CDD), Risk Management, Reporting, Id/Background Checks, Sanction & PEP Screening with Daily Monitoring and Compliance Management			

B



	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/Uni	N/A	N/A	Western Europe	Director of Law and Technology; PhD Students
16.	Interview	Research Institute/Uni	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. FIs, 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 Development Officer; Financial Crime Compliance Lead; Head of Compliance
21.	Conference	Panel inc. FinTech Firms, Payment Providers, Universities, FIs	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. FIs 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 Institutions and Insurance Companies	N/A	N/A	N/A	Detective Sergeant; Solutions Director; Financial Crime Intelligence and Investigations Director and others

B

CODE FRAME

Hot topics &
Frequency analysis

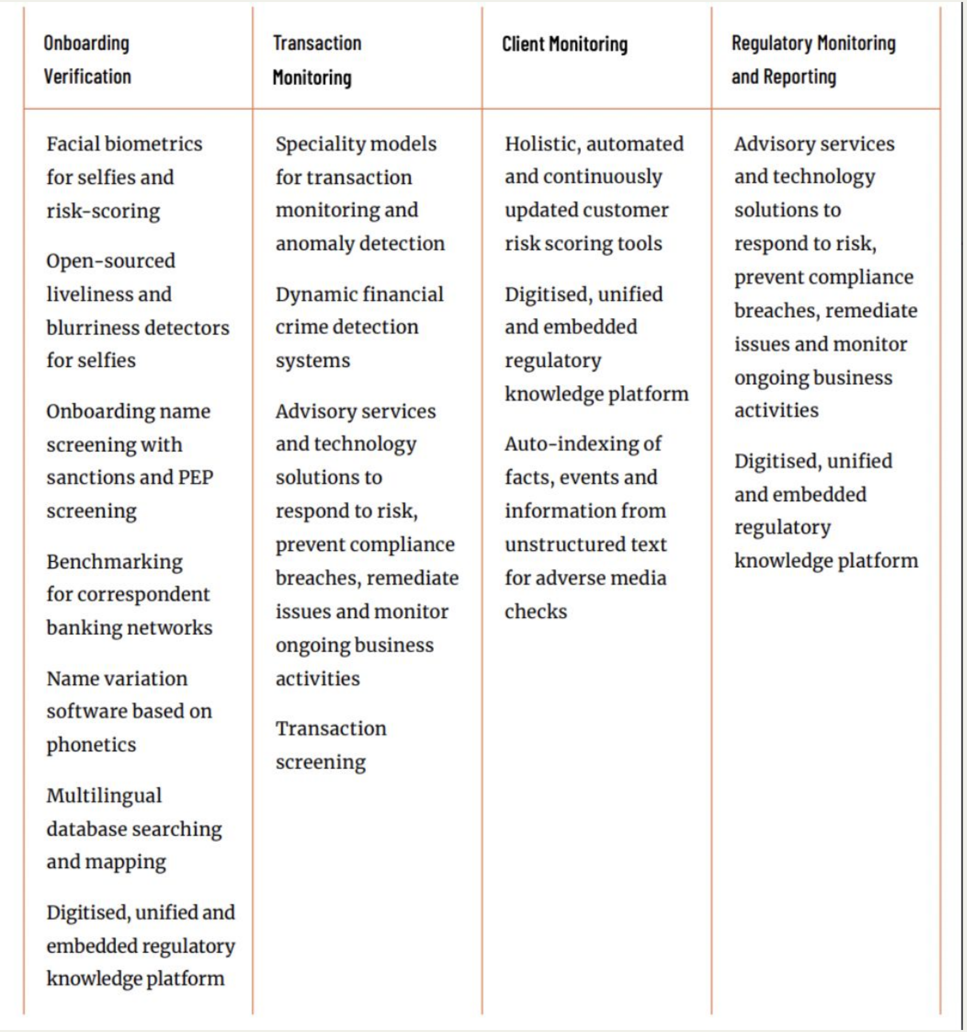
BACKGROUND

- **Business**
  - Area of Focus (7)
  - Philosophy | Goals (14)
  - Product (15)
  - Use / Adopters (14)
- **Underlying Tech**
  - Current Trends (2)
  - AI/ML/DLT Techniques (19)
- **Creation Process**
  - Design, Testing (11)
  - Internal vs External Involvement (13)
  - Impact Assessments (3)
- **Overall Impact**
  - Criteria for NPOs (18)
  - Impact on Lifecycle (2)
  - Impact on NPOs (11)
  - Impact on Financial Inclusion (7)
- **Pipeline/Future Trends (16)**
- **Solutions? (3)**
- **Open Questions (6)**

THEMES

- **Effectiveness, Accuracy, Reliability**
  - Goals (9)
  - Claims (13)
  - Metrics & Case Studies (3)
  - Data Quality (17)
  - Other Difficulties (15)
- **Transparency & Explainability**
  - Transparency / Blackbox (15)
  - Explainability (15)
  - Secrecy (3)
  - Strategic Classification (2)
- **Privacy Protection & Security**
  - Privacy Risks (3)
  - Data Sharing (1)
- **Accountability, Contestability, Oversight, Competence**
  - Human Element (23)
  - Training/Competence (7)
  - Monitoring, Auditing, Oversight (4)
  - Complaints or Appeal Procedures (3)
  - Accountability Split (4)
- **Fairness & Financial Inclusion**
  - Bias, Profiling, Discrimination (14)
  - Accessibility (2)
- **Awareness of Risks & Safeguards (7)**
  - Risk Mitigation (8)

B



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

B

The AML Process

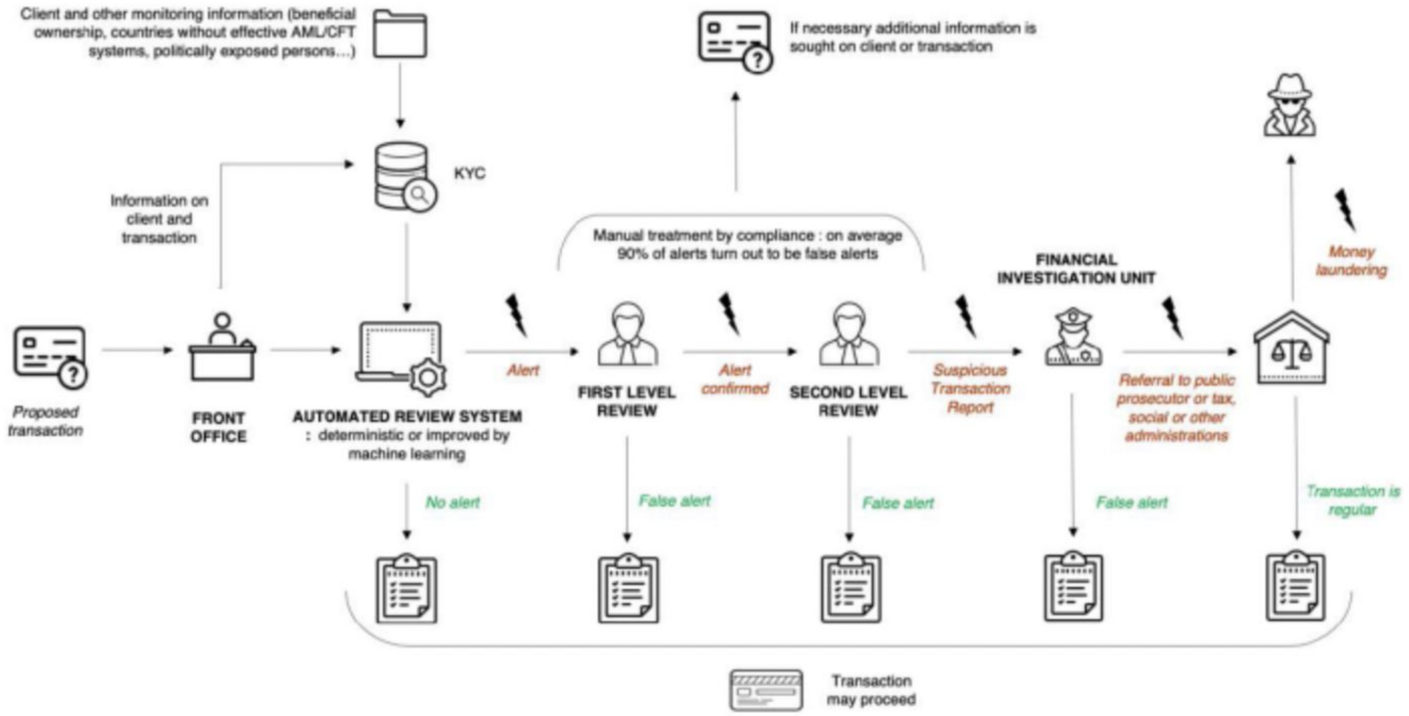
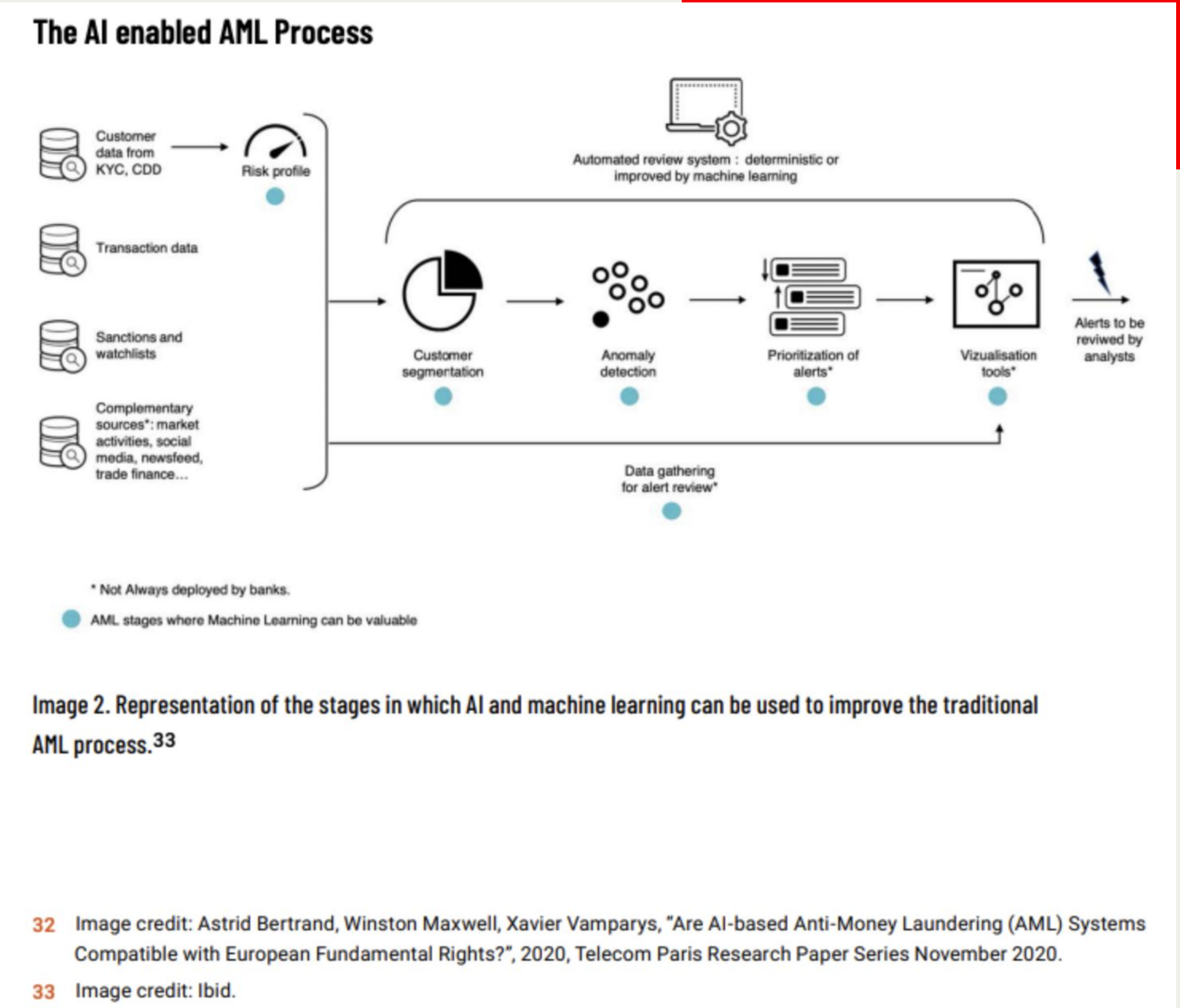

Client and other monitoring information (beneficial ownership, countries without effective AML/CFT systems, politically exposed persons…)
KYC
Information on client and transaction
If necessary additional information is sought on client or transaction
Manual treatment by compliance : on average 90% of alerts turn out to be false alerts
Proposed transaction
FRONT OFFICE
AUTOMATED REVIEW SYSTEM : deterministic or improved by machine learning
Alert
FIRST LEVEL REVIEW
Alert confirmed
SECOND LEVEL REVIEW
Suspicious Transaction Report
FINANCIAL INVESTIGATION UNIT
Referral to public prosecutor or tax, social or other administrations
Money laundering
No alert
False alert
False alert
False alert
Transaction is regular
Transaction may proceed

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



The AI enabled AML Process

Customer data from KYC, CDD
Risk profile
Transaction data
Sanctions and watchlists
Complementary sources*: market activities, social media, newsfeed, trade finance...
Automated review system : deterministic or improved by machine learning
Customer segmentation
Anomaly detection
Prioritization of alerts*
Vizualisation tools*
Alerts to be reviwed by analysts
Data gathering for alert review*
* Not Always deployed by banks.
● AML stages where Machine Learning can be valuable

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.

B