Vol. 02 No. 02 (June 2024) ISSN: 2963-220X (p); 2964-626X (e)

aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

Digital Financial Services Effort in Enforcing Anti-Money Laundering through Open Banking Optimization

Ganda Raharja Rusli, Anestia Hayubriandini Fermay*
PT Allo Bank Indonesia Tbk, Indonesia

* Corresponding author: anestia.fermay@allobank.com

Keywords:
Anti-Money Laundering,
Digital Financial Services,
Open Banking, Regtech

Abstract

Technology has revolutionized finance, but seamless services increase fraud risks. As digital finance grows, anti-money laundering (AML) systems struggle with high transaction volumes. The main objective of this study is to verify whether open banking catalyzes the efficiency of transaction monitoring in AML. Another objective is to analyze the current agenda of regulators in Indonesia, which is related to the Indonesia Payment Systems Blueprint 2025 and customer data security. The Delphi technique pinpointed contemporary AML compliance technologies, encompassing money laundering, Regulatory Technology, and regulatory bodies. The article delves into a comparative analysis between Regulatory Technology and financial crime, which emphasizes several actions to eradicate money laundering, such as strengthening the AML system, customer screening, and allowing cross-data sharing between institutions. In addition, this paper explores RegTech's limitations and forthcoming hurdles regarding AML compliance. The finding shows that open banking catalyzes the efficiency of transaction monitoring in AML and supports the regulator's agenda to combat money laundering with some requirements.

Submitted: 28 October 2023
Accepted: 31 May 2024
Published: 1 June 2024

***To cite this article*:** Rusli, G. R. & Fermay, A. H. 2024. *Digital Financial Services Effort in Enforcing Anti-Money Laundering (AML) through Open Banking Optimization*. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2(2):159-174, https://doi.org/10.59593/amlcft.2024.v2i2.158

Introduction

Connecting banking and financial technology (FinTech) through the interlink of the two services allows small business players to carry out business transactions more efficiently. For instance, support of access to capital and provision of a safe payment system as well as foster economic growth.[1] However, there is an issue related to tracking the customer transaction flow, which is suspected of being involved in suspicious transactions related to money laundering. Financial institutions (FI) do not have the authority to access the same consumer data in different FI's to find out the track record of their financial activities. When the customer's funds have gone out to other FIs, it will not be easy to get a big picture of the transactions carried out by these customers. Therefore, cross-data sharing through open banking is believed to be a solution for enforcing AML efforts in FIs.

[1] (Bank Indonesia, 2019)

Technologies in this context pertain to the tools and systems designed for streamlining and automating financial services. Essentially, digital financial services are innovative solutions in financial services that include electronic cash, crowdfunding platforms, and virtual currencies (VCs), among others, which have emerged over recent years. The European Commission (2019)[2] has identified sectors and products susceptible to money laundering risks. These involve cash transactions, the financial sector, the gambling industry, non-financial businesses and their products, fund transfers carried out by nonprofit organizations, and some new sectors with unique products. Combating financial crime necessitates collaboration between regulators, who must work efficiently together.

Financial Institutions (FIs) require Regulatory Technology (RegTech) solutions to enhance AML Compliance[3] while improving Transaction Monitoring capabilities[4] and understanding how best to integrate RegTech into their operations.[5] Certain components from previous analyses raise questions about data sharing's role in AML/CFT efforts against terrorism financing. Consequently, a cooperative model between governance and regulated FIs has been developed where these institutions share data for AML/CFT purposes, but it would not be possible without RegTech development.[6] The alliance of FIs and technology companies[7] or public-private stakeholders[8] is essential for such developments.

The regulator had established a data sharing policy through 27, 2022, on Personal Data Protection (Indonesian: *Undang-undang Pelindungan Data Pribadi*, or UU PDP)[9]. Cross-data sharing is permissible, as written in Article 15, paragraph 1 (point d, the clause on the interests of supervision of the financial services sector). It is stated that the rights of the personal data subject, as referred to in Article 8, article 9, article 10 paragraph (1), article 11, and Article 13, paragraphs (1) and (2), are excluded from supervision of the financial services sector, monetary, payment systems, and system stability finances carried out in order state administration. UU PDP also supports the central bank of Indonesia's agenda related to the Indonesia Payment System Blueprint 2025 (SPI 2025).[10] The Blueprint consists of five payment system visions towards 2025 for implementation by five working groups, namely Open Banking, Retail Payment System, Large-Value (Wholesale) Payment System and Financial Market Infrastructure, Data and Digitalization, as well as Regulatory, Licensing and Supervisory Reforms. SPI 2025 ensures a

[2] European Commission, "Report From The Commission To The European Parliament And The Council," *Angewandte Chemie International Edition, 6(11)* (2019): 951–952. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0370&from=GA.

[3] Dirk A. Zetzsche et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation," *SSRN Electronic Journal*, (2017), https://doi.org/10.2139/ssrn.3018534.

[4] Dionysios S. Demetis, "Fighting Money Laundering with Technology: A Case Study of Bank X in the UK," *Decision Support Systems* 105 (2018): 96–107, https://doi.org/10.1016/j.dss.2017.11.005.

[5] Emily Lee, "Financial Inclusion: A Challenge to the New Paradigm of Financial Technology, Regulatory Technology and Anti-Money Laundering Law," *SSRN Electronic Journal*, (2018): 1–51, https://doi.org/10.2139/ssrn.3018960.

[6] Douglas W. Arner, Jànos Barberis, and Ross P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation," *Northwestern Journal of International Law and Business* 37, no. 3 (2017): 373–415; Dong Yang and Min Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations," *Emerging Markets Finance and Trade* 54, no. 14 (2018): 3256–71, https://doi.org/10.1080/1540496X.2018.1496422.

[7] R. Butler, T. and Brooks, "On the Role of Ontology-Based RegTech for Managing Risk and Compliance Reporting in the Age of Regulation," *Journal of Risk Management in Financial Institutions* 11, no. 1 (2017): 19–33.

[8] K. Lai, "Blockchain as AML Tool: A Work in Progress," *International Financial Law Review, London*, 2018.

[9] 27th, 2022 on Personal Data Protection (UU PDP), https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022 accessed on August 6, 2023.

[10]Indonesia Payment System Blueprint 2025, https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx accessed on July 22, 2023.

balance of innovation through the Implementation of Know Your Customer (KYC) and AML/CFT.

This paper aims to ascertain how open banking enhances the efficiency of transaction monitoring in AML. It also seeks to examine Indonesia's current regulatory agenda regarding Indonesia Payment Systems Blueprint 2025 and customer data security. Compared to the previous study conducted by Arner et al. (2017), which used regulators and policymakers as their survey subject, this study focuses on specific stakeholders who are Compliance AML experts with intensive experience in the finance and banking industry over five years.

This study centered on facts and contemporary advancements and findings about financial crime cases, particularly emphasizing the scourge of money laundering. In addition, the paper explains RegTech and its relevance to cross-data sharing related to open banking. Then, research on the emergence of new technologies in the finance and banking sector, particularly FinTech and RegTech, has facilitated a deeper comprehension of how innovation enables financial institutions to develop cutting-edge solutions. Properly managing data has become increasingly critical as it is a valuable resource for these advancements. Finally, the study proposes recommendations on technologies that will play a major role in AML transaction monitoring by optimizing open banking.

The Delphi method was utilized to identify recent technologies for AML compliance, including money laundering, Regulatory Technology, and regulators. The paper discusses the comparison between Regulatory Technology and financial crime and the constraints and future challenges of RegTech for AML compliance. This research is exploratory, and the approach used in this exploratory study was the Delphi method, which was developed by the RAND Corporation (RAND, 2019).[11] This iterative methodology relies on the insights of specialists who respond to a series of recurring surveys to prognosticate and anticipate forthcoming trends within a designated industry or topic. The Delphi method pursued four distinct objectives during this research:

1. Recruit a minimum of six experts in AML compliance and RegTech who are engaged in or employed by financial institutions to address matters related to anti-money laundering.
2. Determine the prevailing elements that AML compliance experts consistently emphasize when utilizing RegTech and other cutting-edge technologies.
3. Shift the focus towards future implications of RegTech implementation on the evolution of money laundering in the medium to long term and
4. To strive for a comprehensive accord (alternatively called "consensus") among AML compliance and RegTech experts regarding a collection of actions that regulatory bodies could deem essential objectives in the battle opposed to financial crime.

At least six experts had to be recruited to make this research relevant. At the end of the hiring process, six AML compliance or RegTech professionals confirmed they could participate in this study and be part of the panel of experts. According to the research conducted,[12] a minimum of five panels were necessary to ensure realistic results. Therefore, the recruitment of six specialists was deemed sufficient despite initially contacting over 10 experts. The aim was to maintain a relatively small panel size to guarantee high response and retention rates, as Delphi surveys require strong participant commitment. Google Forms were the tools for data collection. Two phases comprised one survey, each enough to get consensus among the surveyed experts. Otherwise, a third phase with an additional survey would have been necessary. The first phase (called *"Phase 1"*) included open and wide questions on the relevance of RegTech for AML compliance. The second phase (called *"Phase 2"*) included more technical questions and was elaborated using the results from the first survey.

[11] Delphi method, www.rand.org/topics/delphi-method.html.

[12] Esman Kurum, "RegTech Solutions and AML Compliance: What Future for Financial Crime?," *Journal of Financial Crime* 30, no. 3 (2023): 776–94, https://doi.org/10.1108/JFC-04-2020-0051.

Participants, all experts or with considerable experience in AML compliance or RegTech solutions in digital financial services, were hired via message on Gmail. A paper and weblink were sent to each participant for each phase via email to access the survey, and reminders were sent via email to non-responders. Survey questions included free-text answers for Phase 1, Likert scales, and multiple-choice questions for Phase 2. Therefore, the collected data were both qualitative and quantitative. Sufficient time was needed for respondents, and two weeks were given to the panel of experts to submit their answers, from August 5 to August 19, 2023, for Phase 1, and two weeks, from August 20 to September 5, 2023, for Phase 2. Such timelines had to be established to streamline the entire research process and allow professionals ample time amidst their busy schedules.

The Exploitation of Technologies within Digital Financial Services

The Federal Reserve Bank of St. Louis reports that digital banking fraud increased during the COVID-19 pandemic.[13] Additionally, a report by Business Insider Intelligence found that account takeover fraud (when hackers gain unauthorized access to an account) has increased by over 280% since 2015.[14] The escalation of digital banking fraud can be attributed to five primary factors, namely:

1. Technological advancements like digital payment systems like QRIS have made online transactions more accessible and convenient. However, it represents new threats, such as fake QRIS codes. The QRIS code generated by malefactors could potentially direct victims to fraudulent web pages that mimic authentic login portals for digital banking or social media platforms.
2. Weak cyber security or lack of strong authentication protocols leads to several digital banking systems continuing to depend on feeble authentication protocols, such as passwords or PINs, which are susceptible to brute-force attacks and social engineering strategies. Consequently, financial institutions must allocate resources toward implementing more robust authentication techniques like biometric authentication and multi-factor authentication (MFA) to enhance the security of their online banking systems.
3. Lack of regulatory compliance, like inadequate customer identification and verification procedures, is the gate for fraudsters to open accounts using fake identities or stolen information. Weaknesses in security protocols, such as inadequate authentication measures, may also lead to unauthorized access to customer accounts. Additionally, a lack of regulatory oversight or failure to comply with regulations may result in vulnerabilities exploited by fraudsters.
4. The increasing sophistication of fraudsters using machine learning and artificial intelligence. One technique used is Natural Language Processing (NLP). With NLP techniques, fraudsters utilize chatbots to communicate with bank customers and smuggle money. The other technique is Generative Adversarial Networks (GANs), which fraudsters use to generate synthetic data-like bank accounts like real ones, not to stimulate suspicion from regulatory bodies.
5. Insider threats such as employee negligence, employee misconduct, and third-party risk contribute to the insider threats that FIs face if they are not regularly audited and implement strict internal controls.

There is a strong correlation between fraud and money laundering. Fraud often involves the illegal acquisition of funds, which are then laundered through various means to conceal their

[13]https://www.stlouisfed.org/on-the-economy/2022/sep/fed-guidelines-master-account-access-payment-services accessed on July 22, 2023.

[14]https://www.businessinsider.com/capitol-one-data-breach-has-heavy-implications-2019-7 accessed on July 22, 2023.

illicit origins. In this sense, fraud and money laundering are two sides of the same coin, with one often leading to or facilitating the other. The Indonesian Government's steadfast dedication to combatting money laundering has been evidenced by the outcomes of its recent decision of the Constitutional Court Number 15/PUU-XIX/2021 on the results of the judicial review of Article 74 of Law Number 8 of 2010 on Prevention and Eradication of Money Laundering (Money Laundering Law) which has established legal certainty and ensured uniformity in the interpretation and enforcement of anti-money laundering regulations.

Talking about the exploitation of technologies in digital financial services can be seen in several cases, such as Danske Bank's Extonian branch,[15] where billions of euros were laundered through non-resident accounts. Another example is the case of Latvia's ABLV Bank[16], which was accused by US authorities of facilitating large-scale criminal activity and became subject to sanctions. Other instances include investigations into potential money laundering activities at German online bank N26 and UK-based Revolut.[17]

In 2021, N26 had been fined for weak anti-money laundering controls and received another warning from the German financial regulator, BaFin. It happened due to deficiencies in its AML systems. Meanwhile, Revolut, known as a *"borderless financial super app,"* offers many services a consumer would associate with a bank. Revolut case related to sanctions, they claimed that their system could detect and automatically halt transactions to individuals who matched against the sanctions list. However, the system only flagged the transaction for further investigation but still allowed the transaction to go through. As a result, Revolut's systems failed to pick up the mass fraud, allowing thieves to steal USD 20 million from the company's cash.

Regulatory Technology (RegTech) and Its Relevancy with Cross-Data Sharing

From the money laundering and fraud cases explained above, system deficiency can be loopholes that hamper the FIs, and it contributes to their financial and reputation risk. Especially if the system implementation does not comply with the standards provided by the regulators. The compliance process that RegTech can automate includes customer due diligence, transaction monitoring, and reporting. This can assist financial institutions to comply with regulations more efficiently and effectively, reducing the risk of errors and punitive actions. According to the Institute of International Finance (IIF), RegTech can encompass auditing, reporting, compliance tools (like KYC and AML/CFT implementation), and risk management. This can be achieved by connecting advanced algorithms and business models, artificial intelligence, machine learning, and real-time supervision. Given the nature of the present digital financial era, which heavily relies on data and is characterized by high velocity, large variety, and a significant volume of data (referred to as the 3V), these aspects are highly likely to operate and evolve.[18]

The main contributions focus on RegTech, essentially merging regulation and technology. RegTech solutions drive digitalization and digital innovation, affecting vast swaths of organizations, entities, and authorities, providing the means to improve areas such as digital reporting, potentially upturning preexisting structures, and reshaping regulatory processes and

[15] European Parliament, "Money Laundering - Recent Cases from a EU Banking Supervisory Perspective," no. February (2018): 1–24, https://www.europarl.europa.eu/cmsdata/142725/EGOV Briefing on EU Banking supervisory perspective.pdf.

[16] European Parliament.

[17] Dermot The, "BIROn - Birkbeck Institutional Research Online The Politics of FinTech: Technology , Regulation and Disruption" 99 (2021): 859–72, https://eprints.bbk.ac.uk/id/eprint/43244/10/43244a.pdf.

[18] Henrik Braun, "Evaluation of Big Data Maturity Models: A Benchmarking Study to Support Big Data Maturity Assessment in Organizations," 2015, 129, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1t4LKpN2EAxU8KbkGHQ3SCOcQFnoECA4QAQ&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F196555414.pdf&usg=AOvVaw3ng3KVN2-0l5wiXhkHFZ91&opi=89978449.

systems.[19, 20] The data-driven will introduce new or shift current paradigms, moving, for example, from a Know Your Customer (KYC) to a Know Your Data (KYD) approach.[21] The data ecosystem emerges as a key aspect[22] where data are shared *"among regulators, industry associations, and investors, which is the foundation for integrated technology-driven regulation."*[23] Data can be structured (such as trade orders and canceled orders, market data, and customer portfolio) or unstructured (such as emails, voice recordings, social media profiles, or other communications), qualitative or quantitative, and granular or aggregated.[24]

Cross-data sharing with good infrastructure and secure access is essential to optimize the implementation of RegTech among FIs, regulators, industry associations, and investors. Currently, cross-data sharing between FIs has already happened for payment systems, and the implementation of QRIS is one example of open banking. It is consistent with the BSPI, which shows the central bank's role in supporting interoperability, competition, and innovation, as well as the operation of public infrastructure. The open banking initiative through open application programming interface (API) standardization and integrated payment interface (IPI) aims to encourage digital transformation in banking and promote interlinks between FinTech and banks.

The idea of cross-data sharing in transaction monitoring to enforce AML can mirror how the central bank of Indonesia standardizes the API and IPI so that data exchange between FIs and regulators can be safely secured. The advantage that FIs and regulators can obtain from implementing open banking for transaction monitoring in AML is that the fraudulent activities can be adequately managed with inter-access between FIs, regulators, and any institution linked to the activities. It will make the investigator work more effectively and efficiently in investigating cases related to money laundering.

[19] Douglas W. Arner et al., "Sustainability, FinTech and Financial Inclusion," *European Business Organization Law Review* 21, no. 1 (2020): 7–35, https://doi.org/10.1007/s40804-020-00183-y.

[20] Petros Kavassalis et al., "The Journal of Risk Finance an Innovative RegTech Approach to Financial Risk Monitoring and Supervisory Reporting Article Information," *The Journal of Risk Finance* 19, no. 1 (2018): 1–18, https://doi.org/10.1108/JRF-07-2017-0111.

[21] Arner, Barberis, and Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation."

[22] Seán O'Riain, Edward Curry, and Andreas Harth, "XBRL and Open Data for Global Financial Ecosystems: A Linked Data Approach," *International Journal of Accounting Information Systems* 13, no. 2 (2012): 141–62, https://doi.org/10.1016/j.accinf.2012.02.002.

[23] Yang and Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations."

[24] EIOPA, "Digital Transformation Strategy," Yang and Li, "Evolutionary Approaches and the Construction of Technology-Driven Regulations." 2021.

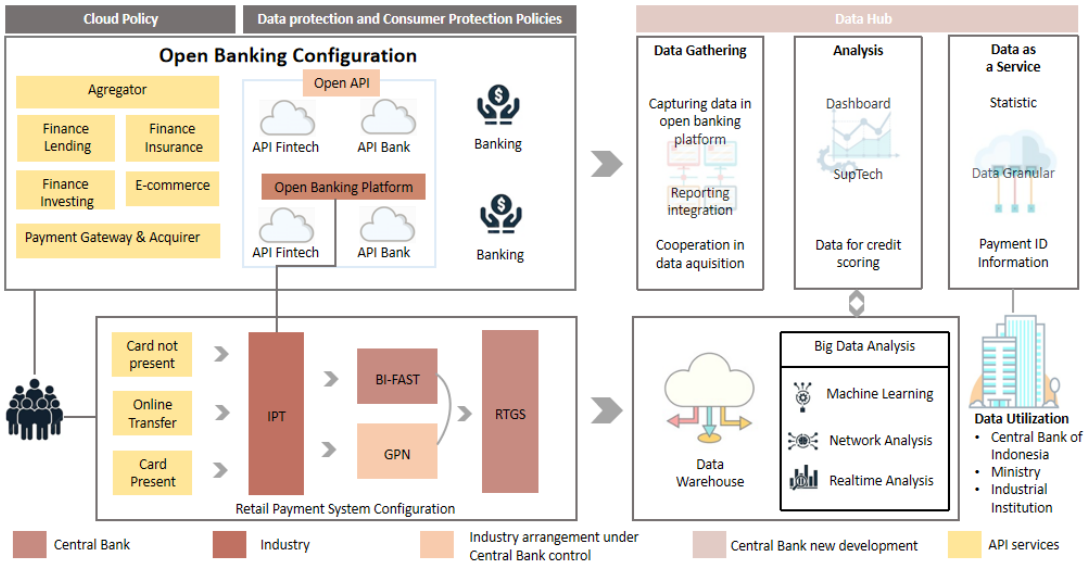

Figure 1. Open API SNAP Data-Hub Configuration
Source: Bank Indonesia, 2021

Open API Payment Standard (SNAP) is a set of protocols and instructions that facilitate interconnection between applications in processing payment transactions stipulated by the Central Bank of Indonesia. SNAP QRIS itself is the embodiment of the (SPI) 2025 in addition to the existing platforms, namely Open API, BI-FAST, QRIS, IPT, BI-RTGS, Data Hub, Payment ID, Sandbox 2.0, and electronically as enablers for the three sectors, namely economic sector, financial sector, and Bank Indonesia itself.

SNAP, on the other hand, as Open API positions itself as a middle system as a bridge for data communication between the front end and the back end that acts as an enabler or data hub to carry out transactions between central bank network systems in various ASEAN+ countries to carry out transaction settlements.

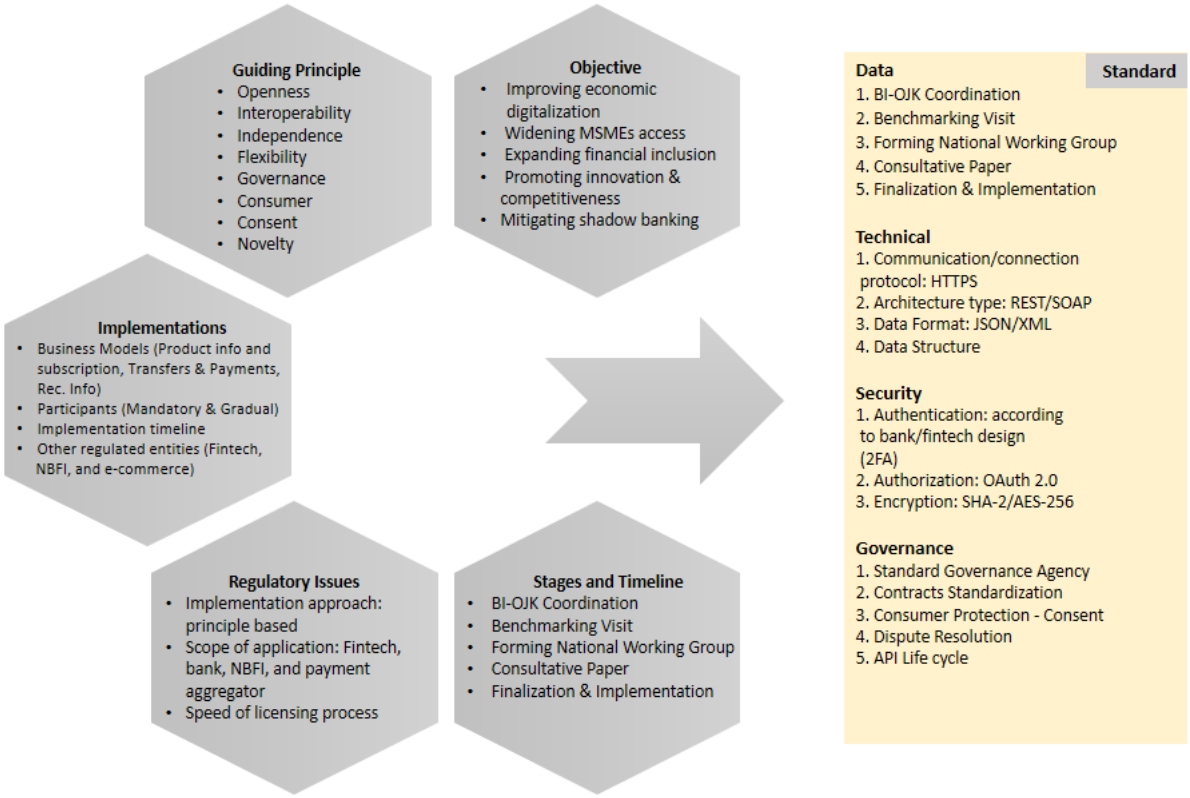

Figure 2. Open API Standard Policy Framework
Source: Bank Indonesia, 2021

In implementing SNAP as an Open API, a framework foundation must be adhered to as a governance standard to become an Open API reliable, sustainable for development in the future, and safe for use. Open banking implementation aims to support digital transformation in banking to become more seamless and integrated. As a result, it became the catalyst for banking in standardizing Open API concerning data standards, technical guidelines, levels, security standards, and good governance. Banks must keep their existence by providing services and various financial services/FinTech startups.

Open Banking to Optimize AML Transaction Monitoring

Using antiquated systems, such as obsolete (AML) solutions may result in financial institutions suffering losses that could have otherwise been averted through AI-powered analysis and big data. Consequently, banks and other financial establishments must embrace contemporary methods that enable them to stay ahead of their processes while ensuring regulatory compliance that guarantees cost-effectiveness and efficiency. The escalation of financial misconduct and the imperative for strengthened cybersecurity protocols have underscored the necessity for RegTech. RegTech solutions in the financial crime sector utilize advanced big data analysis techniques to scrutinize massive amounts of data and establish connections between seemingly unrelated data points, thereby gaining a comprehensive regulatory perspective. This data is accessible via open banking, which establishes a direct connection to the bank for seamless real-time transaction tracking and client risk evaluation.

According to the Delphi survey that was conducted and sent to the experts in AML and Regtech, several RegTech solutions are most likely used. All six participants successfully submitted their answers for the Phase 1 survey, resulting in a response rate of 100 percent. This is acceptable, given that the research required at least five AML or RegTech specialists. The

survey consisted of five open-ended questions, which elicited free-text responses. Therefore, Figure 3 summarizes the results obtained through manual text analysis for each question in Phase 1.

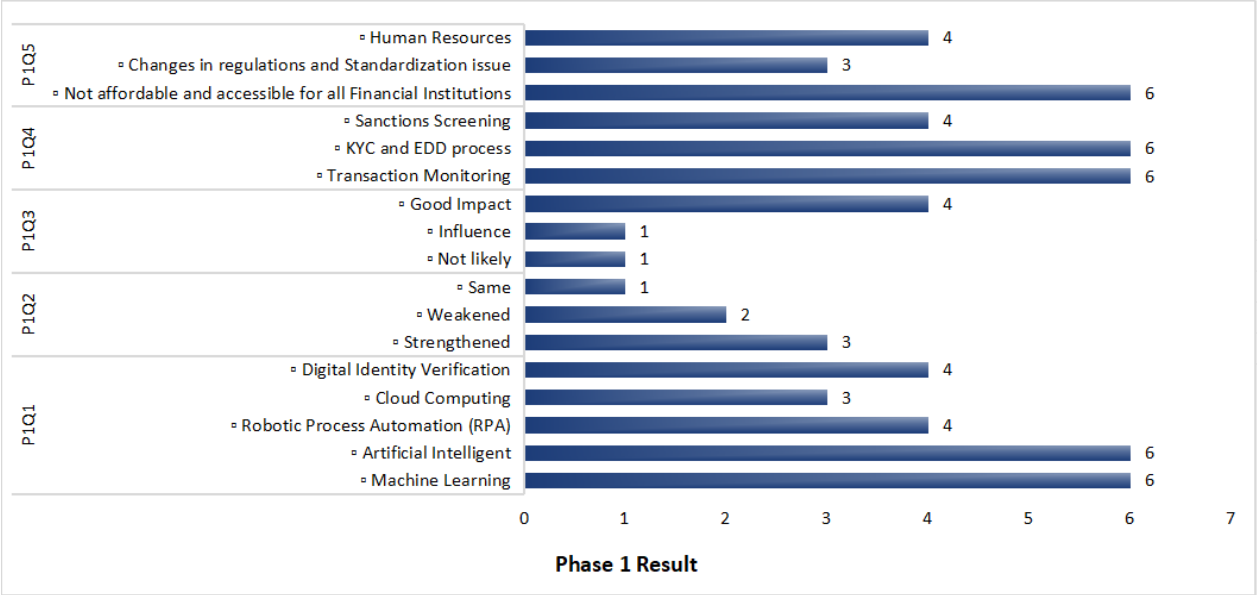

Figure 3. Phase 1 Result

In Phase 2, the response rate was 100%, as all six participants submitted their answers on time. The survey comprised Likert scale questions ranging from 1 (not at all important) to 5 (very important), along with two closed inquiries for the experts' panel to rank their response from Round 1. The survey for this phase was divided into four parts, namely:

1. Advancements in technology for AML compliance;
2. Money laundering, RegTech, and regulators;
3. RegTech versus Financial Crime.; and
4. Constraints and forthcoming obstacles of RegTech for AML compliance.

The purpose of P2Q1 was to ascertain the respondent's perspective on the future focus areas of RegTech solutions concerning AML compliance (Table 1). Question P2Q2 aimed to assess the potential impact of advanced technological implementations by financial institutions in their anti-money laundering (AML) efforts on the complexity level of illicit money laundering techniques adopted by perpetrators, as depicted in Table 2. The objective of P2Q3 was to ascertain whether RegTech solutions have the potential to surpass regulators' suggestions in the realm of AML programs and policy development within financial institutions (as indicated by Table 3). P2Q4 aimed to determine what the panel thinks the next topics to be addressed by RegTech solutions regarding AML compliance will be (Table 4). P2Q4 aimed to ascertain the panel's hierarchy of priorities regarding future challenges in RegTech implementation for AML compliance, as presented in Table 5.

Table 1. Phase 2-Synthesized Answers from Experts to Question 1 (P2Q1)

P2Q1: Below is a compilation of technologies that participants in Round 1 have identified as having the greatest potential to impact AML compliance programs over the next decade significantly. Please rate your perception of the significance each technology will have on AML compliance within the next ten years, utilizing a rating system from 1 ("Not at all important") to 5 ("Very important")

Answer from expert Technologies	Not important at all [1] in %	Unimportant [2] in %	Neutral [3] in %	Important [4] in %	Very Important [5] in %
Machine Learning (P2Q1.1)	-	-	-	50%	50%
Artificial Intelligence (P2Q1.2)	-	16.7%	-	33.3%	50%
Robotic Process Automation (RPA) (P2Q1.3)	16.7%	-	50%	-	33.3%
Digital Identity Verification (P2Q1.4)	-	-	-	50%	50%
Cloud Computing (P2Q1.5)	-	-	16.7%	33.3%	50%

Consensus was reached for each of the questions in Phase 2, except for the first question (P2Q1) about robotic process automation, which was considered less likely to significantly impact the AML compliance program due to the percentage being less than 50%. The strongest consensuses among participants for each topic discussed at the end of Phase 2 are explained as follows:

a. Machine Learning and digital identity verification are rated as the most impactful technologies in the AML compliance program (100%), followed by artificial intelligence and cloud computing (83.3%). These changes are changing how digital financial services identify customers using digital identity verification and automating daily manual assignments using machine learning.

Table 2. Phase 2- Synthesized Answers from Experts to Question 2 (P2Q2)

P2Q2: To what extent do you believe that the employment of advanced technological systems by financial institutions for their anti-money laundering (AML) compliance procedures will impact the complexity of money laundering tactics employed by criminals? (one answer possible)

Response options	Experts Answer, in %
Money Laundering methods will become more sophisticated	100%
Money Laundering methods will become less sophisticated	-
Money Laundering methods will remain the same	-

b. Implementing advanced technologies in AML compliance programs will inevitably prompt a corresponding increase in the sophistication of money laundering techniques, reaching full capacity at (100%). It is an alert to digital financial services to increase the AML system capability to be relevant to technology development. In addition, by leveraging the technology, the system can detect and scrutinize potential anomaly behavior related to money laundering.

Table 3. Phase 2-Synthesized Answers from Experts to Question 3 (P2Q3)

P2Q3: In the future, will RegTech solutions possibly wield a more substantial impact than regulatory bodies on formulating anti-money laundering (AML) policies in financial institutions? (one answer possible)

Response options	Experts Answer, in %
Yes	83.3%
No	16.7%

c. RegTech solutions have been confirmed to have a more significant influence than regulators on how AML policies are designed within FIs (83.3%). However, regulators possess the authority to regulate and steer the AML policy. Failure to do so may result in RegTech taking over this role, which, if utilized improperly, can adversely affect unbiased decision-making.

Table 4. Phase 2: Synthesized Answers from Experts to Question 4 (P2Q4)

P2Q4: Below is a compilation of the topics that have been identified as potential focus points in financial crime by respondents from Phase 1. RegTech solutions may aid in addressing these concerns. Please indicate your level of agreement with the significance of implementing RegTech solutions for each topic using a rating scale from 1 ("Not at all important") to 5 ("Very important")

Answer from expert Technologies	**Not important at all [1] in %**	**Unimportant [2] in %**	**Neutral [3] in %**	**Important [4] in %**	**Very Important [5] in %**
Transaction Monitoring (P2Q4.1)	-	-	16.7%	-	83.3%
KYC and EDD process (P2Q4.2)	-	-	-	33.3%	66.7%
Sanctions screening (P2Q4.3)	-	-	-	-	100%

d. Sanction screening (100%) is listed as the most likely to become the next focus point in financial crime that RegTech solutions could help to counter. In addition, transaction monitoring and KYC and EDD processes also have the potential that RegTech solutions tackle in the future respectively (83.3%, 66.7%). Sanction screening has garnered significant attention in this sector, given the nature of digital financial services in offering foreign exchange services. This is to ensure that their reputation remains untarnished, and they do not engage with any counterparts who are sanctioned or blacklisted.

Table 5. Phase 2: Synthesized Answers from Experts to Question 5 (P2Q5)

P2Q5: Below is a compilation of constraints cited by Round 1 participant as the primary obstacles to implementing RegTech solutions in financial institutions for AML compliance. Please rate the significance of each constraint using a rating scale from 1 ("Not at all important") to 5 ("Very important")

Answer from expert Technologies	Not important at all [1] in %	Unimportant [2] in %	Neutral [3] in %	Important [4] in %	Very Important [5] in %
Not affordable and accessible for all Financial Institutions (P2Q5.1)	-	-	16.7%	50%	33.3%
Changes in regulations and Standardization issue (P2Q5.2)	-	16.7%	16.7%	50%	16.7%
Human Resources (P2Q5.3)	-	16.7%	33.3%	16.7%	33.3%

e. The implementation of RegTech solutions has the specific challenge confirmed by the respondents as non-affordable and accessible for all financial institutions (83.3%), and changes in regulations and standardization issues (66.7%) become the second limitation of it and at last, followed by the human resources (50%). The varying size of digital financial services has resulted in differing capacities to offer comprehensive RegTech solutions, owing to differences in their inherent capital and budgetary eligibility. Nonetheless, this should not pose a significant obstacle if regulators provide specific guidance and policies to ensure compliance among digital financial services.

Table 6. Group Mean Response for Questions P2Q1, P2Q4, and P2Q5

Questions	Response Options	Group Mean Response (1-5)	Mean absolute deviation (MAD)
P2Q1	Machine Learning (P2Q1.1)	4.5	0.5
	Artificial Intelligence (P2Q1.2)	4.2	0.8
	Robotic Process Automation (RPA) (P2Q1.3)	3.8	0.9
	Digital Identity Verification (P2Q1.4)	4.8	0.3
	Cloud Computing (P2Q1.5)	4.3	0.7
P2Q4	Transaction Monitoring	4.7	0.6

	(P2Q4.1)		
	KYC and EDD process (P2Q4.2)	4.7	0.4
	Sanctions screening (P2Q4.3)	5	0
P2Q5	Not affordable and accessible for all Financial Institutions (P2Q5.1)	4.2	0.6
	Changes in regulations and Standardization issue (P2Q5.2)	3.7	0.8
	Human Resources (P2Q5.3)	3.7	1

In the Phase 1 survey, text analysis and text mining affirmed that advanced technologies such as machine learning, artificial intelligence (AI), robotic process automation (RPA), cloud computing, and digital identity verification are poised to significantly impact AML compliance within financial institutions. As per the experts surveyed, these have been presented as response options for Phase 2 to prioritize and rank their thoughts. In this section, the data analysis is more focused on Phase 2 because the analysis of replies to Phase 1 is the source of the design survey for Phase 2.

The Delphi method relies on the potential for surveyed experts to reach a consensus on specific topics through anonymous responses to successive surveys. To ensure accurate analysis of collected data and raw results, it was necessary to establish a consensus definition for this study. Consensus was deemed achieved for categorical values (i.e., yes-no questions) when over 50% of participants provided the same response. For scales and ratios (such as Likert scales ranging from 1 to 5), consensus was considered reached when the group mean response fell within the intervals of [1;2] or [4;5].

Phase 2 data analysis focused on categorical values for yes-no and closed-ended questions (P2Q2, P2Q3) (Tables 3, 4) and the calculation of group mean responses for scales and ratios (P2Q1, P2Q4, P2Q5). Categorization was available to question 2 (P2Q2) to proceed with data analysis. Regarding questions 2 and 3 of Phase 2 (P2Q2, P2Q3), consensus was reached in both cases, with 100% and 83.3% agreement, respectively. This means that the growing use of RegTech solutions by financial institutions for AML compliance will lead to more technologically sophisticated money laundering methods, and RegTech solutions will have a greater influence than regulators' recommendations on how AML policies are designed within financial institutions.

Furthermore, Mean Absolute Deviation (MAD) is a quantitative measure gauges the degree of variation in each data set relative to its mean. The computation involves averaging the absolute differences between each value and the mean. A smaller MAD suggests that the data points are tightly clustered around their central tendency, whereas an elevated MAD indicates greater spread or dispersion. A lower MAD implies proximity to the mean and reduced variability, which may suggest dependability, consistency, or uniformity; conversely, a higher MAD signifies a significant deviation from the mean and amplified variability that could indicate noise, instability, or heterogeneity.

According to the group means responses in Table 6 for questions P2Q1, P2Q4, and P2Q5, Financial institutions are advised to consider investing in RegTech solutions as a means of strengthening their anti-money laundering compliance programs using digital identity verification for sanction screening, machine learning, and artificial intelligence for transaction

monitoring, KYC and EDD process. Furthermore, FIs must prioritize investing in RegTech solutions to bolster their capacity to adapt to emerging technologies and expedite the maturation of their AML compliance program. Indeed, the sooner FIs enhance their AML compliance technology, the better it catalyzes the implementation of open banking in terms of technology infrastructure readiness.

Conclusion

Implementing outdated systems, such as archaic (AML) solutions, can lead to financial institutions incurring losses that could have been prevented using AI-powered analysis and big data. Henceforth, banks and other financial establishments must adopt modern approaches to stay ahead of their operations while ensuring regulatory compliance, cost-effectiveness, and efficiency. The data analysis showed that using advanced technologies such as machine learning and digital identity verification as part of RegTech solutions catalyzes the efficiency of transaction monitoring and KYC and EDD processes in AML. It also supports the strategy and plan of regulators to combat money laundering and how AML policies are designed within financial institutions. Furthermore, the respondents suggested enhancing transaction monitoring, sanction screening, KYC, and EDD processes would be the next issue RegTech solutions could cover.

It has been shown that time will become an ever more crucial resource for FIs to integrate RegTech solutions to stay on top of regulatory changes related to open banking and get ahead of any upcoming developments. As FIs combat the same fraudsters and money launderers, working cooperatively supported by cross-data sharing enabled by open banking will improve the FI's environment in terms of providing safety and soundness for banks and the integrity of the international financial system. Regulators must remain aware that criminals are employing increasingly sophisticated methods for money laundering. As such, regulators should monitor RegTech and embrace technology more fully to enhance their oversight capabilities. This necessitates recruiting additional technical specialists who can assist with the seamless integration of RegTech into regulatory frameworks.

Acknowledgment

On behalf of the Allobank, the author would like to thank everyone for making this study possible and for their continued support of the Allobank in its research endeavors. Further, we would like to thank the following individuals: Rika Astari (RegTech.ID), Pandu Adiat (Allobank), Muhammad Iqbal Saksono (ALAMI, former Head of AML CFT - SeaBank), Christian PYK (Bank Sinarmas, former AML CFT Lead - SeaBank), Kemal M (SeaBank), and Robby Julian (SeaBank) for their contributions and willingness to participate as a respondent to make this study possible.

In particular, we are grateful to Indra Utoyo (President Director of Allobank, Dimas Hananto Nugroho (Head of Compliance & AML/CTF Allobank), and Dewi Evarini (AML/CTF Dept Head Allobank) for their valuable effort and support throughout the study.

References

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley. "FinTech, RegTech, and the Reconceptualization of Financial Regulation." *Northwestern Journal of International Law and Business* 37, no. 3 (2017): 373–415.

Arner, Douglas W., Ross P. Buckley, Dirk A. Zetzsche, and Robin Veidt. "Sustainability, FinTech and Financial Inclusion." *European Business Organization Law Review* 21, no. 1

(2020): 7–35. https://doi.org/10.1007/s40804-020-00183-y.

Bank Indonesia. *Indonesia Payment Systems Blueprint 2025 Bank Indonesia: Navigating the National Payment Systems in the Digital Era BA*, 2019.

Braun, Henrik. "Evaluation of Big Data Maturity Models: A Benchmarking Study to Support Big Data Maturity Assessment in Organizations," 2015, 129. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj1t4LKpN2EAxU8KbkGHQ3SCOcQFnoECA4QAQ&url=https%3A%2F%2Fcore.ac.uk%2Fdownload%2Fpdf%2F196555414.pdf&usg=AOvVaw3ng3KVN2-0l5wiXhkHFZ91&opi=89978449.

Butler, T. and Brooks, R. "On the Role of Ontology-Based RegTech for Managing Risk and Compliance Reporting in the Age of Regulation." *Journal of Risk Management in Financial Institutions* 11, no. 1 (2017): 19–33.

Commission, European. "Report From the Commission to the European Parliament and The Council." *Angewandte Chemie International Edition, 6(11), (*2019): 951–952., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0370&from=GA.

Demetis, Dionysios S. "Fighting Money Laundering with Technology: A Case Study of Bank X in the UK." *Decision Support Systems* 105 (2018): 96–107. https://doi.org/10.1016/j.dss.2017.11.005.

EIOPA. "Digital Transformation Strategy," 2021.

European Parliament. "Money Laundering - Recent Cases from a EU Banking Supervisory Perspective," no. February (2018): 1–24. https://www.europarl.europa.eu/cmsdata/142725/EGOV Briefing on EU Banking supervisory perspective.pdf.

Kavassalis, Petros, Harald Stieber, Wolfgang Breymann, Keith Saxton, and Francis Gross. "The Journal of Risk Finance An Innovative RegTech Approach to Financial Risk Monitoring and Supervisory Reporting Article Information." *The Journal of Risk Finance* 19, no. 1 (2018): 1–18. https://doi.org/10.1108/JRF-07-2017-0111.

Kurum, Esman. "RegTech Solutions and AML Compliance: What Future for Financial Crime?" *Journal of Financial Crime* 30, no. 3 (2023): 776–94. https://doi.org/10.1108/JFC-04-2020-0051.

Lai, K. "Blockchain as AML Tool: A Work in Progress." *International Financial Law Review, London*, 2018.

Lee, Emily. "Financial Inclusion: A Challenge to the New Paradigm of Financial Technology, Regulatory Technology and Anti-Money Laundering Law." *SSRN Electronic Journal*, (2018): 1–51. https://doi.org/10.2139/ssrn.3018960.

O'Riain, Seán, Edward Curry, and Andreas Harth. "XBRL and Open Data for Global Financial Ecosystems: A Linked Data Approach." *International Journal of Accounting Information Systems* 13, no. 2 (2012): 141–62. https://doi.org/10.1016/j.accinf.2012.02.002.

The, Dermot. "BIROn - Birkbeck Institutional Research Online The Politics of FinTech : Technology, Regulation and Disruption" 99 (2021): 859–72. https://eprints.bbk.ac.uk/id/eprint/43244/10/43244a.pdf.

Yang, Dong, and Min Li. "Evolutionary Approaches and the Construction of Technology-Driven Regulations." *Emerging Markets Finance and Trade* 54, no. 14 (2018): 3256–71. https://doi.org/10.1080/1540496X.2018.1496422.

Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner, and Janos Nathan Barberis. "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation." *SSRN Electronic Journal*, no. January (2017). https://doi.org/10.2139/ssrn.3018534.