DOI: https://doi.org/10.36719/2789-6919/20/35-37

Zamina Hasanli
Baku State University
master student
hasanleezamina@gmail.com

HOW FINTECHS CAN ADDRESS AML CHALLENGES

Abstract

This paper discusses the impact of hyper-digitalisation brought about by the COVID-19 pandemic on the financial services industry, creating new opportunities but also posing significant challenges in detecting financial crime risks. Financial institutions are faced with the increasing burden of regulatory compliance, internal pressures, and demands for seamless customer experiences. Anti-money laundering professionals are particularly affected, with limited resources and inefficient manual processes that hinder their ability to detect illicit activities. In response, fintechs are using technology to reimagine banking and offer solutions to these challenges. This paper highlights the need for the financial industry to embrace innovation and collaborate with fintechs to effectively manage financial crime risks.

Keywords: *AML (Anti-Money Laundering), Digital ID, Cryptocurrency, Regulatory Compliance, Customer Onboarding*

Zəminə Həsənli
Bakı Dövlət Universiteti
magistrant
hasanleezamina@gmail.com

“Fintech”lər çirkli pulların yuyulması ilə mübarizə problemlərini necə həll edə bilər?

Xülasə

Bu məqalədə COVID-19 pandemiyasının yaratdığı hiper-rəqəmsallaşmanın maliyyə xidmətləri sənayesinə təsiri, yeni imkanlar yaradılması, eyni zamanda maliyyə cinayətləri risklərinin aşkar edilməsində əhəmiyyətli problemlərin meyadana çıxması müzakirə ediləcək. Maliyyə institutları artan tənzimləyici komplayns yükü, daxili təzyiqlər və qüsursuz müştəri təcrübəsi tələbləri ilə üzləşirlər. Çirkli pulların yuyulması ilə mübarizə üzrə peşəkarlar xüsusilə məhdud resurslar və qeyri-qanuni fəaliyyətləri aşkar etmək qabiliyyətinə mane olan səmərəsiz avtomatlaşdırılmamış proseslərin təsirinə məruz qalırlar. Buna cavab olaraq, fintechlər bankçılığı yenidən formalaşdırmaq və bu çətinliklərə həll yolları təklif etmək üçün texnologiyadan istifadə edirlər. Bu sənəd maliyyə sənayesinin innovasiyaları mənimsəməsi və maliyyə cinayətləri risklərini effektiv şəkildə idarə etmək üçün fintech-lərlə əməkdaşlıq edilməsi ehtiyacını vurğulayır.

Açar sözlər: *çirkli pulların yuyulması ilə mübarizə, Rəqəmsal identifikator, Kriptovalyuta, Komplayns, Müştəri monitorinqi*

Introduction

To justify investments in AML control systems, improving customer experience is critical. High costs and poor processes increase AML risk. Digital verifications of entities and individuals are replacing physical and paper-based ones, but there is no global standard, making it inconvenient and inaccurate. Digital ID interoperability is urgently needed for faster, cheaper, and more accurate eKYC. The EU's eIDAS regulation recognizes electronic IDs from its 27 member countries, allowing cross-border electronic transactions with trust and interoperability (1).

Various players in the financial industry, such as fintechs, exchanges, and traders, are encountering more intricate regulations. Payment Service Providers (PSPs) are heavily regulated and face scrutiny for sanctions screening and transaction monitoring. In the UK, the Payment Services Regulation 2017 has brought PSPs under scrutiny. Similarly, the Monetary Authority of Singapore has provided guidelines for PSPs, while European supervisory authorities have issued guidance to prevent terrorist financing and money laundering in electronic fund transfers. Cryptocurrency firms, including exchanges, traders, and asset managers, are growing rapidly and present a budding financial crime threat. Cryptocurrency's anonymity makes it susceptible to sanctions evasion, financing terrorism, and other illegal activities. PayPal now accepts payments in cryptocurrency, and in 2020 launched a new service enabling customers to buy, hold and sell cryptocurrency from their PayPal accounts (2).

Governments and regulators worldwide are struggling to keep up with the growing cryptocurrency ecosystem. The Financial Action Task Force (FATF) has prioritized cryptocurrency and emphasized the importance of financial crime prevention. The "Travel Rule" extends anti-money laundering obligations to cryptocurrency transfers above a certain threshold and applies to Virtual Asset Service Providers (VASPs) (3). In the US, virtual currencies are recognized as a significant financial innovation but are also viewed as a preferred form of payment for illegal activities. The Office of Foreign Assets Control (OFAC) has targeted the cryptocurrency ecosystem due to the increasing exploitation of virtual currency by bad actors in sanctioned countries. In the European Union, the Crypto Travel Rule has been mandated, and the Digital Services Act (DSA) and Digital Markets Act (DMA) have been proposed to create a safer and more open digital space (4).

Regulators worldwide are trying to keep up with the expanding cryptocurrency ecosystem. The Financial Action Task Force (FATF) has prioritized cryptocurrency and reiterated the importance of financial crime compliance and prevention. The "Travel Rule" extends AML/CFT obligations to cryptocurrency transfers valued at US$1,000 or more. In the US, FinCEN recognizes virtual currencies as a substantial financial innovation but also views them as a preferred form of payment for illegal activities (5). The European Commission has proposed two legislative initiatives to reform the EU's digital economy, the Digital Services Act (DSA) and the Digital Markets Act (DMA), applicable across the whole EU to create a safer and more open digital space. The DSA sets rules on the liability of digital platforms for the content, products, and advertisements they distribute. Lenders need to comply with customer due diligence measures and be registered with the FCA for money laundering supervision. The "regulatory sandbox" approach encourages experimentation while allowing states to oversee and evaluate what companies are trying to do (6).

New technology can help AML compliance executives improve customer experience, manage risk, and navigate regulatory challenges. Fintech companies are rapidly introducing intuitive, economical, and scalable products that leverage social media and data integration to gain market share and disrupt traditional financial services. Big tech companies like Amazon, Apple, Facebook, and Google have set high standards for digital experience, which now apply to financial services. To keep up, traditional financial institutions are launching digital products, creating fintech incubators, and considering M&A and strategic investments in fintechs (7).

To create effective AML compliance frameworks, companies should focus on five core elements. The first is customer onboarding, which involves effective customer screening, KYC, and enhanced due diligence. Digital onboarding can improve efficiency and the customer experience, but all checks should be auditable. Key questions to consider include identifying fraudulent documents, confirming the person's identity and uncovering any risks associated with the entity (8).

Ongoing monitoring is essential for companies to comply with AML regulations beyond customer onboarding. It helps to identify potential risks as they occur, and ongoing checks are necessary to assess these risks. It's important to ensure that the right alerts are received from the screening dataset and that they are accurately recorded in the customer record. Some questions to consider include whether the alerts are appropriate and how they are reflected in the customer's overall record (9).

Continuing to monitor customer transactions is crucial. It is necessary to ask questions such as: Is a customer making payments to a sanctioned entity? Is a customer at risk of fraud? Has a customer account been compromised?

Continuous KYC: Keeping track of changing customer information is a crucial aspect of KYC compliance. Financial institutions must be aware of the data points that should trigger a new KYC process. This involves considering factors such as the importance given to specific data points, the initial risk score, and other relevant factors. Questions to consider include: Does our current onboarding tool help us monitor changes in customer circumstances? If an address change triggers an ID verification process, does our system request an ID with the new address and conduct a liveness check? (10).

Customer risk score is determined by various factors. It is essential to gather all relevant information and integrate each system's machine-readable output into the risk engine regularly. This ensures that the customer experience aligns with any potential risk identified.

Conclusion

Fintechs have become a major player in the financial industry, but their growth has been hindered by Anti-Money Laundering (AML) challenges. With the increasing regulatory pressure, fintechs are facing the need to comply with AML laws to maintain their credibility and reputation. However, with the help of technology, fintechs have the opportunity to address these challenges and streamline their compliance processes. Fintechs can leverage innovative technologies such as machine learning, artificial intelligence, and blockchain to enhance their AML compliance processes. These technologies can assist in identifying and verifying customer identities, detecting suspicious transactions, and improving overall transaction monitoring.

References

1. https://iclg.com/practice-areas/fintech-laws-and-regulations/usa
2. https://www.digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
3. https://www.legislation.gov.uk/uksi/2017/752/contents/made
4. https://www.mas.gov.sg/regulation/payments/key-notices-and-guidelines-for-payment-service-providers
5. https://www.eba.europa.eu/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers
6. https://www.fatf-gafi.org/documents/
7. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
8. https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf
9. https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf
10. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Received: 16.02.2023 Accepted: 30.03.2023