CURRENCY BRIDGE

Knowing How to Manage KYC & KYT for FinTech

Knowing How to Manage KYC & KYT for FinTech

Table of Content

1. Introduction

Know Your Customer ("**KYC**") and Know Your Transaction ("**KYT**") are critical components of Anti-Money Laundering ("**AML**") and Countering the Financing of Terrorism ("**CFT**") regulations that fintech companies must adhere to. KYC involves verifying the identity of customers to prevent fraud and money laundering, while KYT focuses on monitoring transactions to detect and prevent illicit activities.

2. KYC and KYT Requirements for Fintech Companies: Trends, Costs, and Challenges

The trends in KYC compliance for fintech companies in 2024 highlight a significant shift towards advanced technologies and streamlined processes. Fintech firms are increasingly adopting artificial intelligence ("**AI**"), machine learning ("**ML**"), and blockchain to enhance identity verification and fraud detection capabilities. There is also a notable move towards document-free verification methods, such as liveness detection and passive biometry, which improve security and user convenience. Regulatory frameworks are tightening, requiring continuous updates to KYC requirements to meet evolving standards. Additionally, integrated KYC and transaction monitoring platforms are emerging as essential tools to balance operational efficiency and compliance costs

3. Costs of Compliance

Compliance with KYC and KYT regulations is costly. The expense stems from implementing sophisticated verification systems, maintaining ongoing monitoring, and ensuring data security. For instance, the average cost per KYC check for banks globally was approximately $2,613 in 2023, a significant increase from previous years[1]. This expense can be particularly burdensome for smaller fintech firms, which may lack the financial resources of traditional banks. As these firms grow and acquire more customers, the cumulative compliance costs increase, potentially affecting their profitability. When Fintech firms allocate a significant portion of their resources to compliance, it may reduce the ability to invest in technologies and services that could enhance their competitive edge.

[1] https://www.dataleon.ai/en/blog/kyc-trends-in-fintech-2024-embracing-digital-compliance

4. Trends in KYC and KYT Compliance

Below are three (3) trends that we think deserve mentions.

Advanced Technologies. Fintech companies are increasingly adopting advanced technologies such as AI and ML, and blockchain to enhance KYC processes. AI and ML improve the accuracy of identity verification and detect fraudulent activities more efficiently. According to a report by Juniper Research, the adoption of AI in KYC processes can reduce compliance costs by up to 45% by 2023. These technologies enable real-time analysis of large datasets, identifying patterns and anomalies that manual processes might miss. For example, AI algorithms can cross-reference customer data against global watchlists, ensuring compliance with international sanctions and AML regulations. Blockchain technology, on the other hand, provides an immutable record of transactions, enhancing the transparency and security of financial operations.

Document-Free Verification. There is a shift towards document-free verification methods, which streamline the onboarding process and reduce friction for customers. Techniques like liveness detection and passive biometry are becoming more common, enhancing security and user convenience. A study by PWC indicated that 73% of customers prefer seamless digital onboarding experiences. Document-free verification methods, such as facial recognition and fingerprint scanning, not only speed up the process but also improve accuracy and reduce the risk of identity theft. Liveness detection ensures that the biometric data provided is from a live person and not a spoof. Passive biometry, which involves capturing biometric data without active participation from the user, further enhances user experience by making the process quick and unobtrusive.

Regulatory Tightening. Regulatory frameworks are becoming stricter, requiring fintech companies to continuously update their KYC and KYT protocols. The Sixth Anti-Money Laundering Directive (6AMLD) in the EU and the Corporate Transparency Act (CTA) in the US are examples of regulations that mandate detailed customer due diligence and transaction monitoring. These regulations impose significant penalties for non-compliance, with fines reaching up to €5 million or 10% of annual turnover under 6AMLD. The tightening of these regulations reflects a global trend towards greater transparency and accountability in financial transactions. Fintech companies must invest in robust compliance systems to avoid penalties and maintain customer trust. This trend also highlights the importance of staying abreast of regulatory changes and adapting quickly to new requirements.

5. Challenges in Compliance

Integration of Technology. Integrating advanced technologies like AI and blockchain with existing systems can be complex and costly. According to a report by MarketsandMarkets, the global AI in fintech market size is projected to grow from $3.3 billion in 2020 to $22.6 billion by 2025, at a CAGR of 41.0% during the forecast period. This rapid growth reflects the increasing reliance on AI to enhance security, streamline operations, and improve customer experience. However, ensuring these systems are user-friendly while maintaining high security standards is a significant challenge. The complexity of integration often requires specialized skills and substantial investment, which can strain the resources of fintech companies.

Data Security and Privacy. As fintech companies adopt remote onboarding processes, the risk of fraud and data breaches increases. According to the Identity Theft Resource Center, data breaches in the financial sector increased by 19% in 2021 compared to the previous year. Implementing robust security measures to protect customer data while complying with privacy regulations is essential. The General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US impose stringent requirements on how companies handle personal data, with penalties for non-compliance reaching up to 4% of annual global turnover or $20 million, whichever is higher. These regulations necessitate significant investments in cybersecurity infrastructure and continuous monitoring to ensure compliance.

Operational Efficiency. Balancing the cost of compliance with operational efficiency is a major challenge. Compliance-related costs for financial institutions are estimated to have increased by over 60% over the past decade, according to a Thomson Reuters report. This increase is driven by the need for more sophisticated monitoring tools and the requirement to keep up with evolving regulatory standards. All-in-one platforms that integrate KYC checks with transaction monitoring are emerging as a solution to improve efficiency and compliance. These platforms leverage automation and AI to streamline processes, reduce manual intervention, and enhance accuracy. For example, a report by Juniper Research predicts that AI-driven regtech solutions could save financial institutions up to $1 billion annually by 2024 by reducing compliance costs and improving efficiency.

6. Penalties for Non-Compliance

Non-compliance with KYC and KYT regulations can result in severe penalties, including hefty fines and reputational damage. For example, in 2023, Binance was fined over $4.3 billion[2] for inadequate

[2] https://www.reuters.com/technology/judge-approves-binance-43-billion-guilty-plea-us-seeks-modify-founder-zhaos-bond-2024-02-23/#:~:text=Feb%2023%20(Reuters)%20%2D%20A,the%20world's%20largest%20cryptocurrency%20exchange.

KYC and AML controls, and Poloniex faced a $7.6 million fine for sanctions violations[3]. These penalties underscore the importance of adhering to regulatory requirements. hese penalties underscore the critical importance of adhering to regulatory requirements to avoid significant financial and reputational harm.

Singapore, known for its robust regulatory framework and commitment to financial integrity, has also seen significant enforcement actions related to non-compliance with KYC and KYT regulations.

Wirecard Scandal: In 2020, the Monetary Authority of Singapore ("**MAS**") took enforcement action against Wirecard entities in Singapore. MAS directed Wirecard to cease its payment services in the country after discovering significant regulatory breaches, including inadequate KYC measures. This case highlighted the stringent enforcement of compliance regulations in Singapore and served as a warning to other financial institutions operating in the region.

Credit Suisse Fine: In 2018, MAS imposed a fine of SGD 700,000 on Credit Suisse for breaches related to AML and CFT (Counter Financing of Terrorism) requirements. The fine was part of a broader crackdown on financial institutions that failed to implement robust KYC measures, following investigations into the 1MDB scandal. This enforcement action demonstrated Singapore's commitment to maintaining high standards of compliance and transparency in its financial sector.

Bank J. Safra Sarasin: In 2020, Bank J. Safra Sarasin was fined SGD 1 million by MAS for lapses in AML and CFT controls. The bank failed to establish adequate customer due diligence measures, which led to the facilitation of suspicious transactions. This case further illustrated the importance of stringent compliance practices and the consequences of failing to adhere to regulatory requirements.

The penalties imposed for non-compliance in Singapore serve as a stark reminder of the serious consequences that financial institutions face when they fail to meet regulatory standards. Hefty fines

[3] https://www.wsj.com/articles/crypto-exchange-poloniex-to-pay-7-6-million-to-settle-probe-into-sanctions-violations-7985a009

can significantly impact financial stability, reducing profitability and diverting resources away from critical areas such as innovation and customer service. Additionally, non-compliance can severely damage an institution's reputation, leading to a loss of customer trust and potential business declines. In a highly competitive market like Singapore, maintaining a strong reputation is crucial for attracting and retaining clients.

Enforcement actions often require institutions to overhaul their compliance frameworks, leading to operational disruptions. This can involve extensive audits, staff retraining, and the implementation of new technologies, all of which can be costly and time-consuming. Moreover, institutions found in breach of compliance regulations may face increased scrutiny from regulators, leading to more frequent inspections and audits. This ongoing scrutiny creates an additional operational burden and necessitates continuous improvements in compliance practices.

7. Importance of Strong AML and CFT Controls

Strong AML and CFT controls are vital for fintech companies as they offer multiple critical benefits. Firstly, effective AML and CFT measures help prevent money laundering and terrorist financing, thereby protecting the financial system's integrity. Secondly, compliance with these regulations builds trust with customers, investors, and partners, which is crucial for business growth and sustainability. Lastly, adhering to AML and CFT regulations helps fintech companies avoid severe legal penalties and the associated financial and reputational damage.

8. Role of Technology as an Enabler

Technology is a crucial enabler in complying with AML and CFT regulations. As mentioned earlier in this report, AI and ML algorithms can play a significant role in enhancing identity verification and transaction monitoring. These technologies can analyze vast amounts of data in real-time, identifying patterns and anomalies that may indicate suspicious activities. Blockchain technology also offers substantial benefits for compliance. By providing immutable records, blockchain ensures transparency and trust in financial transactions. Every transaction is time-stamped and cannot be

altered, which aids in verifying the authenticity of transactions and tracing the origin of funds.

Furthermore, integrated KYC platforms can streamline compliance processes, reducing costs and improving efficiency. These platforms consolidate various compliance tasks, such as customer identity verification, transaction monitoring, and reporting, into a single system. This integration reduces the need for manual processes and minimizes errors. A report by Thomson Reuters indicates that financial institutions spend an average of $60 million annually on KYC compliance, with some spending up to $500 million. By leveraging integrated KYC platforms, institutions can significantly cut these costs while maintaining high compliance standards.

9. Relevance to Cryptocurrency

Cryptocurrency also presents unique challenges and opportunities in the context of KYC and KYT. Due to the pseudonymous nature of cryptocurrency transactions, they are particularly susceptible to misuse for money laundering and terrorist financing. Implementing robust KYC and KYT measures in the cryptocurrency space is essential to mitigate these risks.

Regulatory bodies worldwide are increasing scrutiny on cryptocurrency exchanges and wallet providers to ensure they implement effective KYC and KYT measures. For instance, the Financial Action Task Force ("**FATF**") has extended its AML/CFT recommendations to include cryptocurrency transactions, requiring virtual asset service providers to adhere to the same standards as traditional financial institutions. This includes widely known requirement for providers to share the sender and beneficiary information, also known as the 'Travel Rule'.

10. Deterring Crypto-Related Money Laundering and Terrorist Financing

Implementing KYC and KYT measures in the cryptocurrency sector can significantly deter money laundering and terrorist financing:

Identity Verification. Implementing KYC (Know Your Customer) processes in the cryptocurrency sector is a critical measure for deterring money laundering and terrorist financing. KYC processes ensure that cryptocurrency users are who they claim to be, making it harder for criminals to operate anonymously. By verifying the identities of users, exchanges can detect and prevent illicit activities before they occur. This verification process typically involves collecting personal information such as names, addresses, and government-issued identification documents. With verified identities, exchanges can create a more secure environment, reducing the risk of fraudulent activities. For example, according to Persona, effective KYC measures can reduce identity fraud by up to 90%, underscoring the importance of robust identity verification in the cryptocurrency industry.

Transaction Monitoring. KYT measures enable continuous monitoring of cryptocurrency transactions. Advanced analytics and machine learning algorithms can flag unusual patterns and transactions, allowing for timely intervention and reporting of suspicious activities to regulatory authorities. For instance, transaction monitoring systems can analyze transaction volumes, frequency, and geographical locations to identify potentially illicit activities. Castellum.AI reports that

the implementation of KYT measures has led to a significant increase in the detection of suspicious transactions, with some exchanges reporting a 30% improvement in identifying high-risk activities. By monitoring transactions in real-time, exchanges can swiftly respond to potential threats, enhancing overall security.

Cross-Border Collaboration. Cross-border collaboration and information sharing among regulatory bodies can significantly enhance the effectiveness of KYC and KYT measures in the cryptocurrency space. Coordinated efforts help track and intercept cross-border financial crimes, ensuring a safer and more transparent financial ecosystem. International cooperation is essential because cryptocurrency transactions often transcend national boundaries, making it challenging for any single regulatory body to oversee all activities. By sharing intelligence and best practices, countries can collectively improve their defenses against money laundering and terrorist financing. According to Castellum.AI, international collaborative initiatives have led to the successful interception of several large-scale money laundering operations, demonstrating the power of unified regulatory efforts.

11. KYC and KYT Requirements in Singapore

The MAS is the primary regulatory body overseeing AML and CFT compliance in Singapore, including KYC and KYT rea requirements for fintech companies. The MAS has established stringent guidelines to ensure that financial institutions and fintech firms adhere to high standards of due diligence and transaction monitoring.

The MAS Notice 626 requires financial institutions, including fintech companies, to perform Customer Due Diligence ("**CDD**") and Enhanced Due Diligence ("**EDD**") for higher-risk customers. These guidelines mandate that financial institutions must identify and verify customer identities using reliable, independent sources of information. They are also required to perform continuous monitoring of transactions to detect and report suspicious activities is required. Reporting: Institutions must report any suspicious transactions to the Suspicious Transaction Reporting Office promptly. These are some of the requirements amongst others.

12. Conclusion: Perform KYC and Transaction Monitoring with Cost Efficiency Method

While compliance with KYC and KYT requirements poses significant challenges and costs, the adoption of advanced technologies and innovative solutions can help fintech and cryptocurrency companies meet regulatory demands efficiently. These measures not only prevent financial crimes but also build trust and ensure sustainable growth in the fintech sector. In Singapore, adherence to MAS guidelines is crucial for fintech companies to maintain their operations and avoid severe penalties, ensuring a secure and transparent financial ecosystem.

To address these requirements and avoid high initial cost that could derail fintech companies from investing into research and development, they could outsource to Currency Bridge. Currency Bridge already has KYC and KYT modulars that fintech companies or platforms can tap into. This kind of partnership.

Connecting with Currency Bridge

Currency Bridge is a Singapore headquartered turnkey fintech provider, that offers a suite of ready to deploy solutions and SaaS. Our comprehensive products range from KYC to OTC swap and exchange and remittance. Currency Bridge can customize the solution to customers' business.

The team is dedicated to high standards of security and compliance, ensuring our customers can deploy swiftly, meet requirements, and adapt to changing needs! Visit www.currencybridges.com or reach out to sales@sg-qianyi.com to learn more about our services and success stories!