Guardians of Compliance: The role and obligation of Reg-Tech firms towards Criminal Justice Act 2010

Fortify Anti-Money Laundering and Countering the Financing of Terrorism measures.

ABSTRACT

The current global financial landscape is riddled with increased money laundering incidents, resulting in colossal fines imposed on banks worldwide. In response to this, the Irish Government has diligently transposed major EU regulations into national law through the Criminal Justice Act 2010, aiming to fortify Anti-Money Laundering and Countering the Financing of Terrorism measures.

Role of a Reg-Tech company is utmost critical for any to financial institutions, offering a comprehensive suite of solutions to ensure compliance with CJA 2010 regulations. The company's multifaceted approach encompasses cutting-edge technology, including AI-powered mechanisms, and a team of trained analysts committed to meticulous KYC, Due Diligence, and risk identification. Such solutions facilitate early detection of potential money laundering red flags, assist in governance, streamline Suspicious Transactions Reports with advanced algorithms, provide comprehensive training modules, and meticulously screen international financial sanctions, ensuring a robust and compliant framework for financial institutions to effectively combat financial crimes.

GLOSSARY:

1. Anti-Money Laundering Directive (AMLD): A set of regulations issued by the European Union (EU) to combat money laundering and terrorist financing.

2. Anti-Money Laundering: Measures and regulations implemented by financial institutions and governments to prevent, detect, and combat the illegal process of disguising the origins of illicitly obtained money.

3. Beneficial Owners (BO's): The real person who ultimately owns or controls a company or other legal entity, often used to prevent financial crimes like money laundering.

4. Compliance Officer: An individual designated by a financial institution to oversee and ensure adherence to Anti-Money Laundering Directive (AMLD) regulations and related legal requirement.

5. Compliance: The adherence to laws, regulations, internal policies and procedures relevant to the operations of financial institutions, aimed at mitigating risks and ensuring ethical conduct.

6. Counter Terrorist Financing (CTF): Efforts and regulations aimed at preventing terrorist organizations and individuals from rising, moving, and using funds for terrorist activities.

7. Criminal Justice Act 2010 (CJA 2010): Legislation enacted to combat financial crime, including money laundering, terrorist financing, and fraud, by imposing various regulatory requirements and obligations on financial institutions.

8. Due Diligence: The process of conducting thorough investigations and assessments of customers, business partners, transactions, and other counterparties to evaluate their integrity, reputation, and compliance with legal and regulatory requirements.

9. EU Regulations and Directives: Laws and guidelines issued by the European Union (EU) to harmonize regulations across member states and ensure consistency in various areas such as trade, finance, consumer protection, and environmental standards in EU member states.

10. Financial Crime: Illegal activities perpetrated in the financial sector, including money laundering, terrorist financing, bribery, corruption, fraud, insider trading, and tax evasion, posing significant risks to the integrity and stability of the financial system.

11. Financial Intelligence Unit (FIU): A government agency or independent authority responsible for receiving, analyzing and disseminating financial intelligence related to suspicious transactions, money laundering, and terrorist financing activities.

12. KYC (Know Your Customer): A process used by financial institutions to verify the identity of their customers, assess their risk profile, and gather relevant information to prevent money laundering, fraud, and other illicit activities.

13. Money-Laundering Reporting Officer (MLRO): The MLRO is a designated individual within a financial institution responsible for overseeing the institution's compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) regulations.

14. Non European Economic Area (EEA) States: Countries or territories that are not members of the European Economic Area (EEA), which consists of the European Union (EU) member states along with Iceland, Liechtenstein, and Norway. Non-EEA states are not subject to the same laws, regulations, and trade agreements as EEA member states.

15. Politically Exposed Person (PEP): A term used to describe individuals who hold prominent public positions or roles with significant influence or authority, either domestically or internationally. PEPs typically include government officials, high-ranking politicians and heads of state, senior executives of state-owned enterprises, and their immediate family members and close associates.

16. RegTech (Regulatory Technology): It is use of technology, such as artificial intelligence (AI), machine learning (ML) and big data analytics, to streamline regulatory compliance processes within the financial industry.

17. Revenue Department: A government agency responsible for administering and enforcing taxation laws and regulations within a jurisdiction.

18. Risk Management: The systematic identification, assessment, mitigation, and monitoring of risks associated with the operations, products, and services of financial institutions, aimed at safeguarding against potential losses and regulatory non-compliance.

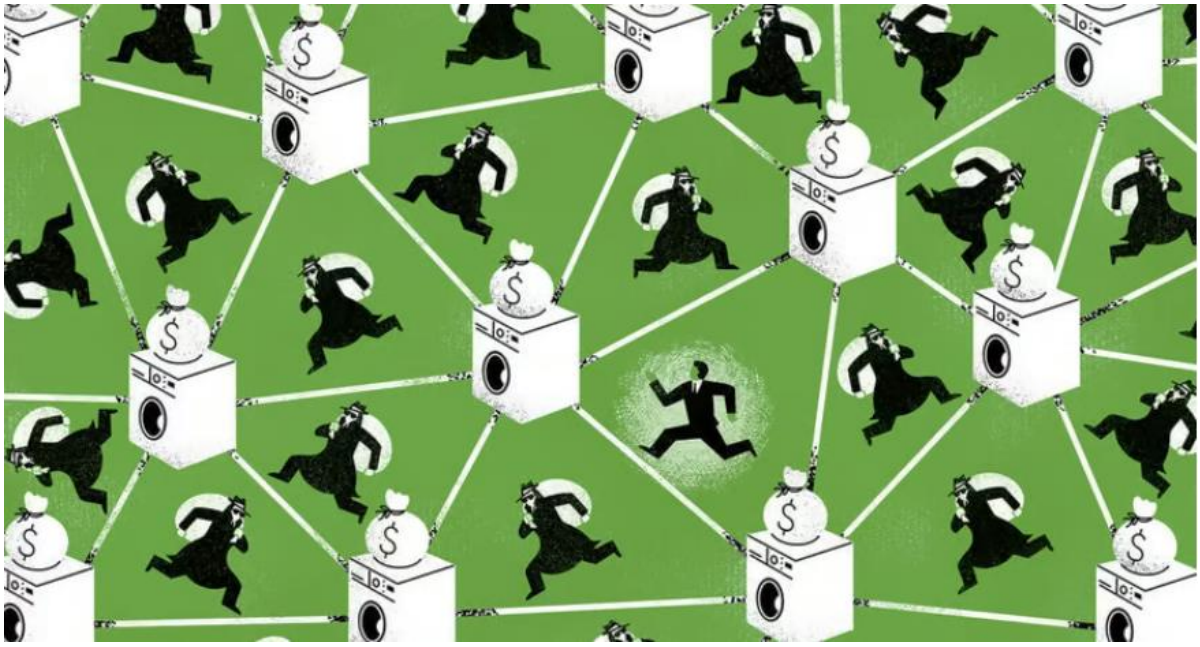
19. Sanctions : Measures imposed by governments or international organizations to enforce compliance with specific laws, regulations, or policies, often related to international trade, human rights, or national security.

20. Suspicious Transaction Reporting (STR): The obligation of financial institutions to report to regulatory authorities any transactions or activities that raise suspicions of money laundering, terrorist financing, or other illicit conduct, enabling authorities to investigate and take appropriate enforcement actions.

21. Three Lines of Defence: A risk management framework comprising three layers of control and oversight within an organization - Operational management, Independent oversight functions, Internal audit.

22. Transaction Monitoring: The continuous surveillance and analysis of financial transactions conducted by customers to detect suspicious activities, such as unusual patterns, high-risk transactions, or potential instances of money laundering or fraud.

CONTENTS



https://www.economist.com/finance-and-economics/2021/04/12

INTRODUCTION

As **The Economist**, a leading business magazine has commented, "Last FY of 2022, the global system for financial crime is hugely expensive and largely ineffective." The global banks around the world were hit with whooping $10.4bn in fines for their failure to curb money-laundering violations. According to Fenergo, there has been an increase of more than 80% in the Money Laundering business since 2019. In the recent past, American bank - Capital One, was fined $390m for failing to report thousands of fishy transactions. The UK witnessed a nasty blow against its leading bank – NatWest with a penalty of £265m for failing to abide by Money Laundering Regulations. In the EU, we have witnessed Danske Bank has failure to identify over $200bn of potentially dirty money washed through the Danish lender's Estonian branch while their top management ignored the red flags.

Considering such global turmoil, the Irish Government has already transposed all major *EU Regulations and Directives* into National Law to combat Money Laundering and Terrorist Financing. A robust framework for *Anti-Money Laundering and Countering the Financing of Terrorism* has been implemented through the *Criminal Justice Act 2010(CJA 2010),* further updated in 2019 with the transposition of *5 AMLD*. The Act ensures that the economy is protected from corruption by illicit funds and allows the smooth functioning of business by avoiding relations with countries having deficiencies in their AML/CFT frameworks.

RISK MANAGEMENT

Primary focus of a Reg-Tech firm , will be to safeguard the interest of the esteemed clients i.e. bank / financial institutions by fulfilling all the obligations and regulatory requirements as laid down in CJA 2010. It must provide complete solution over AML & CTF with our exhaustive coverage on every aspect of *Sec 7 of CJA 2010 and Sec 13 of CJA 2005*. Accurate and structured information will help to meet the KYC and Due Diligence screening with zero tolerance which will help its client to take informed decisions and stay compliant in this evolving landscape.

The applications of the Reg-Tech firm must be well equipped for early detection of any defiance of Money Laundering norms whether there is an attempt to conceal the nature of the business, ownership of the business entity, type of transaction or channels used for the business flow. Their researchers and analysts must perform a thorough screening through state-of-the-art technology combined with human expertise, of every customer data against reliable and reputable available sources - like watch lists, government records and media searches, to screen out clean customers who can bank with you.

Its technology should be backed with adequate AI-powered mechanism to successfully raise red flags for any transaction breach above the threshold or someone trying to conceal by keeping limits lower than the margin. They must maintain strong data warehouses that can filter out all such customers who are *Politically Exposed Person (PEP's),* family members & and their close associates. System must be capable to do deep-check of any customer who might involved with Non-Profit Organizations, State Owned Entities or Enterprises, *High Risk and Cash Intensive businesses* along with the list of all *Beneficial Owners (BO's)* as associated with the business stakeholders.

Strong subject matter experts should be well trained KYC and Due Diligence analysts who are capable to detect any early Risk arising from the *Customer Type*, *Nature of Product* and *Services Dealt* along with the *Transaction Mechanism* through multiple channels and the geographic locations catered by them.

An easy and dynamic data integration platform where every relevant AML & TF update and new emerging risks are categorized and automatically screened against existing firewall to assess the client's risk position. Periodical *Suspicious Transactions* Reporting (STR) from internal agencies and departments as well as risk identified by internal and external auditors should be auto-compiled with an existing data structure to mitigate risk.

Objective of any Reg-Tech company is to enable a De-risking measures delivering 100% guarantee for its client that will always be updated and protected from all AML and TF threats. A dedicated team must always offer exclusive coverage of the regulations and compliance news that help keep its client compliant.

CUSTOMER DUE DILIGENCE

A comprehensive suite of services and products specifically tailored to meet the stringent requirements outlined in *Sections 33-39 of the Criminal Justice Act 2010*, focusing on *Customer Due Diligence (CDD)* for financial institutions.

Core focus of their services revolves around Anti-Money Laundering compliance, aligning with Section 33(1) of the CJA 2010, necessitating customer identification before contractual agreements. Specialized AML tools to facilitate the verification of customer identities, including Politically Exposed Persons, *Non-EEA state individuals*, those from high-risk third countries, and categories defined in *Sections 37-39*. Such process involves ongoing identification, risk assessment, meticulous record-keeping, and trigger-based further due diligence.

"Know Your Customer" forms a fundamental part of CDD, and Reg-Tech firm must provide dynamic document verification and authentication solutions for secure and seamless customer on boarding. These tools enhance identity verification, assess business objectives, scrutinize fund sources, and evaluate potential future risks, effectively reducing fraudulent activities.

Periodical risk management is crucial in CDD, involving risk categorization of customers as high, medium, or low risk based on document and business verification. There is a requirement of strong risk management software with advanced algorithms for effective risk assessment, aiding resource allocation for enhanced due diligence and continuous monitoring of *high-risk* accounts. Their software must conduct routine checks and screening against relevant risk parameters across the customer database.

To comply with the record-keeping requirements of the CJA 2010, Reg-Tech must provide a robust solution for data storage and audit trail management. These tools securely store all CDD-related data, ensuring accessibility for regulatory inspections or audits. The software validates beneficial ownership information with central registrars while maintaining an electronic KYC history for easy retrieval.

Maintaining accurate information about business activity aligns with Section 35(1) of the CJA 2010. Software must be capable to continuously monitor transaction patterns to ensure alignment with intended purposes.

In summary, an ideal Reg-Tech service must include customised services to address AML compliance, KYC, Risk Management, strong record-keeping, business activity monitoring, and international collaboration, ensuring that financial institutions meet CDD requirements as outlined in the CJA 2010.

GOVERNANCE

Having an efficient governance structure is the bedrock of effective AML & TF risk identification and mitigation. Failure to identify risk, insufficient risk management, governance and policies will endanger the reputation of its client's i.e. bank/ financial institutions and might expose them to financial penalties and sanctions.

A customised product development to provide hands-on support plays an immense role in this respect. A full proof system must be enabled to identify and assess risk, effective identification of PEP, assess any correspondence relation with organization and provide instant access to the senior management with a dynamic dashboard and periodical reports. Accordingly, any review and recommendation of policies and procedures passed by the Board of Directors will be incorporated into our system to upgrade the same.

The focused approach to facilitating the *Compliance Officer* will be another key offering wherein periodical training will be conducted especially for the Compliance Officer and related team to assess business risk and discharge his responsibility effectively.

An advanced technology will ensure the *"Three Lines of Defence"* model is executed properly. There will be a smooth flow of information across departments for easy coordination between front-line business units, risk, compliance, and internal audit so that the senior management can review and test any AML controls before launching the same.

SUSPICIOUS TRANSACTIONS REPORTING

Suspicious Transactions Reports (STRs) are the preeminent component against money laundering and terrorist financing. With the help of STRs, the authorities counteract the money laundering and the resulting terrorist financing activities *(Central Bank of Ireland, 2021)*.

There is a critical need for robust financial security against money laundering and terrorist financing activities. Innovative solutions stand as the vanguard in safeguarding client's against such threats by streamlining the process of reporting STRs.

With the ever-evolving landscape of financial crimes, identifying suspicious transactions is vital. Strong product offering must come with comprehensive suite of tools and services to empower financial institutions in detecting and reporting suspicious activities promptly and effectively.

In 2022, many big corporations and banks like *Danske Bank, Credit Suisse*, and *Santander Bank* were fined millions of dollars over anti-money laundering compliance failures, mainly due to inadequate transaction monitoring and failure to report suspicious activity *(RiskScreen, 2023).* Reg-Tech solutions must comply with Section 42(1) of CJA 2010 and help target these issues with efficiency and ease. Cutting-edge algorithms must able to scrutinise transactions without relying on fixed monetary thresholds, adapting to diverse customer behaviours and transaction patterns. There must be a continuous monitoring of

transactions, flagging any deviations or anomalies and enabling proactive detection and reporting.

A simplified reporting mechanism platform allows for the swift and accurate submission of all required information to the *Financial Intelligence Unit (FIU)* and *Revenue Department* using machine learning and artificial intelligence solutions making the system compliant with Sections 42 and specifically 42(2) of the CJA 2010.

Any sensitive data relevant to the transactions and customers must be safeguarded by securing the databases with multiple levels of authentication and approvals. Reg-Tech must provide a dedicated support team to offer ongoing training and assistance to their client's that guarantees to effectively utilize the system, maximising its potential in combating financial crimes.

TRAINING

To stay compliant with Sec 54(6) of CJA 2010, Reg-Tech must focus is to ensure that client's are proficiently trained with the ability to recognize money laundering and terrorist financing risks to detect and prevent unlawful activities.

There should be unwavering commitment towards their client to ensure all employees across departments, job responsibilities and hierarchy possess a thorough understanding of ML & TF risk and stay updated with all relevant legislation and their associated responsibilities. A tailor made training modules to be imparted as per employee department based requirements and conduct periodical refreshers and assessment to ensure employees can identify risks, assess the intensity and report to the right authority as per procedure.

It must ensure that all employees, from new joinee's to the employees handling high-risk departments, are thoroughly trained to deliver their obligations and the company's obligations. It must emphasise the internal reporting procedures including Suspicious Transaction Reports and the role of *MLRO (Money Laundering Reporting Officer)* is relevant to present *Risk Categorisation*. A well-informed and comprehensive training approach will able to keep its client 100% compliant with regulatory guidelines.

INTERNATIONAL FINANCIAL SANCTIONS

Reg-Tech must conduct detailed screening of all *Sanctions*, both diplomatic and economic; to drive policy changes impacting the financial domain. In line with *EU Sanctions Regulations*, it must be responsibility of Reg-Tech firm to track whether any business or trade transactions are being conducted with any sanctioned countries or people listed in the EU Sanction List. If any accidental hit occurs with any such sanctioned countries or persons, then the system must be capable to raise necessary red flags to freeze such accounts and raise a report to the compliance authorities like the Central Bank of Ireland. The Reg-Tech

firm must able to leverage its network reach and ensure all UN Sanctions lists are screened and alerts are raised for their clients across the globe.

Periodical reports of any positive match or potential match must flash in the dynamic dashboard for the senior management to keep them well-informed about the financial sanctions obligations to ensure they have the necessary authority to take further action.

REFERENCES

1. Central Bank of Ireland (2021), 'Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector'. Available at:https://www.centralbank.ie/docs/default-source/regulation/amld-/guidance/anti-money-laundering-and-countering-the-financing-of-terrorism-guidelines-for-the-financial-sector.pdf?sfvrsn=64d4bc1d_11 [Accessed 20 October 2023]

2. Financial Intelligence Unit (2022), 'About FIU Ireland'. Dublin. Available at:https://fiu-ireland.ie/public_documents/aboutFIU.pdf [Accessed 27 October 2023]

3. Financial Intelligence Unit (2022), 'STRs Received'. Dublin. Available at:https://fiu-ireland.ie/public_documents/strs_received.pdf [Accessed 30 October 2023]

4. Department of Justice (2022), 'Suspicious Transactions Reporting'. Dublin: Anti-Money Laundering Compliance Unit. Available at: https://www.amlcompliance.ie/wp-content/uploads/2020/10/FIU-STR.pdf [Accessed 30 October 2023]

5. Department of Justice (2022), 'Suspicious Transactions Reporting'. Dublin: Anti-Money Laundering Compliance Unit. Available at: https://www.amlcompliance.ie/wp-content/uploads/2020/10/Revenue-STR.pdf [Accessed 1 November 2023]

6. RiskScreen (2023), 'The 6 biggest global anti-money laundering fines of 2022'. Available at: https://riskscreen.com/blog/the-6-biggest-global-anti-money-laundering-fines-of-2022/ [Accessed 4 November 2023]

7. https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost . [Accessed 06 November 2023]

8. https://www.clever-soft.com/ . [Accessed 06 November 2023]