Knowledge Sharing Between FIs: Is Sharing STRs the Key to Stronger Financial Security

June-2, 2025

A Suspicious Transaction Report (STR) or a Suspicious Activity Report (SAR) is a document that financial institutions are required to file with the Financial Intelligence Unit (FIU) whenever there is a suspected case of money laundering or financing of terrorism. These reports help monitor activities that appear abnormal and seem like they might have the potential to lead to illegal activities.

Knowledge sharing between FI's (Financial Institutions) regarding STRs or SAR's refers to the practice where different financial institutions share information about suspicious transactions, individuals and entities they identify with each other, allowing them to build

a broader picture of potential money laundering or terrorist financing activities, especially when transactions involve multiple institutions or cross borders, thus enhancing the effectiveness of anti-money laundering (AML) efforts by collaborating and pooling intelligence. However, the sharing of intelligence relating to money laundering or terrorist financing will require consent from the relevant government agencies.

How STRs can help Anti Money Laundering efforts

At an estimated US$2 trillion being laundered each year, money laundering has turned into a global issue. Despite regulatory bodies and Financial Institutions working to combat money laundering world over, the problem seems insurmountable as money laundering spans across jurisdictions, geographies and institutions.

To address this complex issue of money laundering, the Financial Action Task Force (FATF) has recommended that financial institutions should be sharing information between themselves to detect money laundering more easily and comply with the Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) requirements.

The FATF in its 2021 recommendations report states that with technological advances, financial institutions can analyse large amounts of structured and unstructured data and identify patterns and trends more effectively.

Key Takeaways from the FATF on Data Sharing for Anti-Money Laundering:

- Fragmented Customer Data: Customer information is increasingly spread across numerous financial institutions, making it difficult for a single institution to effectively combat financial crime.

- Enhanced Detection through Collaborative Analysis: Sharing data and utilizing advanced analytics across multiple institutions enables the identification of suspicious patterns and activities more readily.
- Improved Risk Management and Compliance: Data sharing strengthens transaction monitoring, risk assessment, customer onboarding, and the identification of beneficial owners.
- Closing Information Gaps: It prevents criminals from exploiting inconsistencies across domestic and international financial institutions.
- Pattern Recognition and Intelligence: Sharing crime typologies and patterns facilitates better crime detection and intelligence-driven investigations.

The type of data that is to be shared between financial institutions includes:

- Customer Due Diligence Information
- Transactions
- Red Flags
- Indications of customer risk
- Updated information of the institutions in a correspondent banking relationship

FATF Recommendations for Effective Data Sharing in Anti-Money Laundering

The FATF emphasizes the importance of open communication between financial institutions, AML/CFT supervisors, and data privacy authorities. This collaboration is crucial for the successful implementation of new technologies and effective data sharing. Regulatory sandboxes (controlled testing environments) offer valuable opportunities to explore how new technologies can align with national and international AML/CFT and data protection laws.

One of the most compelling real-world examples of STR data sharing in action is the Transaction Monitoring Netherlands (TMNL) initiative. Launched in 2020, TMNL is a collaborative effort by five of the largest Dutch banks — ABN AMRO, ING, Rabobank, Triodos Bank, and de Volksbank — to jointly monitor transaction data for signs of money laundering.

This initiative was born out of recognition that criminals often spread their financial activities across multiple institutions, making it difficult for any single bank to detect suspicious patterns. By pooling anonymised transaction data, TMNL allows for cross-institutional analysis, enhancing the ability to detect complex money laundering networks that would otherwise go unnoticed.

Despite initial concerns about data privacy and compliance with the GDPR, the project was able to move forward under the oversight of Dutch regulators and in consultation with the country's Data Protection Authority. TMNL is often cited by the Financial Action Task Force (FATF) and other international bodies as a leading example of how collaborative data-sharing frameworks can improve AML effectiveness while respecting legal boundaries.

Challenges in Using New Technologies:

- Financial institutions find it challenging in sharing information to comply with AML/CFT regulations due to the legal restrictions regarding sharing of customer data.
- Poor data quality, such as inaccurate or outdated information, can undermine the effectiveness of data pooling and lead to unreliable analytical results.
- Insufficient regulatory requirements and guidance hinder the use of new technologies.

The challenges associated with STR data sharing — namely legal restrictions, poor data quality, and limited regulatory guidance — can significantly weaken anti-money laundering efforts. Legal constraints, such as data protection laws, often deter institutions from sharing critical customer information, allowing criminals to exploit regulatory fragmentation by spreading transactions across multiple entities to avoid detection. Meanwhile, poor data quality — such as outdated or inconsistent customer records — undermines the effectiveness of analytics, leading to false positives or missed threats.

The absence of clear regulatory frameworks or guidance on emerging technologies further stifles innovation and collaboration, leaving institutions uncertain about how to proceed and hesitant to adopt new tools. Together, these issues create blind spots in the financial system that sophisticated criminal networks are quick to exploit.

FATF recommends sharing of data using new technologies such as Cryptography/Encryption Technologies and advanced analytics to address the challenges in sharing data.

Questions

1. What is an STR in anti-money laundering? A Suspicious Transaction Report (STR) is a document submitted by financial institutions to the Financial Intelligence Unit (FIU) when a transaction appears to involve potential money laundering or terrorist financing. It's a critical component of global AML compliance frameworks.

2. Why is sharing STR data between financial institutions important? Sharing STR-related data helps financial institutions build a fuller picture of suspicious activity that may span across multiple banks or jurisdictions. This collaboration improves detection, strengthens risk management, and closes information gaps that criminals can exploit.

3. Is data sharing between banks legal under GDPR and similar regulations? Data sharing can be legal if properly anonymised or structured within clear regulatory frameworks. Regulatory sandboxes and close collaboration with data protection authorities are often used to explore compliant ways to share data for AML purposes.

4. What are the key barriers to effective STR data sharing? The main barriers include legal and regulatory uncertainty, inconsistent data quality, siloed systems across institutions, and the lack of standardised technological infrastructure for secure, compliant data exchange.

Quantum Data Engines™

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.

For more details write to: connect@qde.ai