ARTICLE

Tackling financial crime: now is the time to break down silos

The sharing of financial crime intelligence within financial services is often limited and segregated. Technology can bridge the gap between jurisdictions, business lines and departments, whilst saving time on investigations, driving down costs and identifying financial crime typologies. So why do organisations persist in using an outdated, fragmented approach to financial crime risk management?

"These traditional approaches can stifle innovation and create a resistance to change that results in ineffective controls."

Intelligence sharing is the cornerstone of an effective anti-financial crime framework

Amid the Coronavirus pandemic, now more than ever, firms need to find a more effective way to share intelligence on financial crime to ensure they maintain effective controls and mitigate risks.

The Financial Conduct Authority has stated that criminals are taking advantage of the current situation and targeting firms' systems through fraud and exploitation schemes[1].

The Financial Action Task Force (FATF) is also driving an effective information sharing initiative, highlighting that sharing information is essential for the effective identification, mitigation and management of money laundering/ terrorist financing (ML/TF) risk[2].

The unintended consequences of a legacy approach

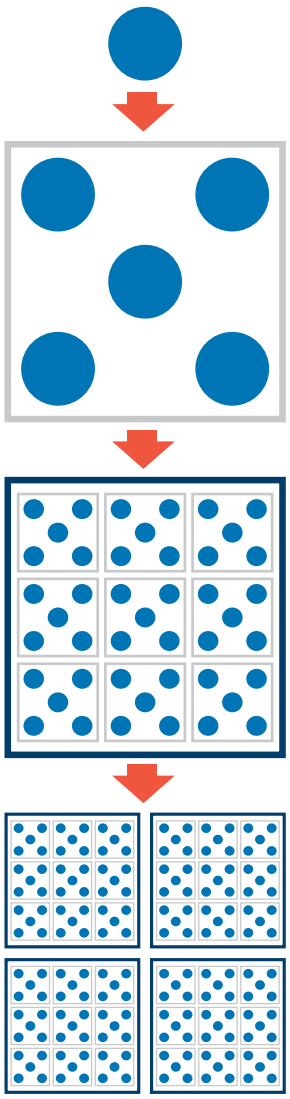
Financial Crime Compliance (FCC) strategy is often based on continuity, governed by traditional silos and powered by legacy technology that results in path dependency. These traditional approaches can stifle innovation and create a resistance to change that results in ineffective controls.

1 https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation
2 https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

For many organisations, responsibilities to identify and investigate potential financial crime risks are broken down into specialisms such as Bribery and Corruption, Sanctions or Fraud. These FCC teams are then segregated according to the line of business and geographical location in which they and their respective customers operate. In the context of larger financial institutions, this can include operations across 60+ jurisdictions and multiple business lines.

Segregation is intended to create specialism and focus to increase efficiency. However, there are unintended consequences of breaking work down into its smallest component parts. It can foster a silo mentality that results in significant delays and incorrect decisions across financial crime investigations. Time, energy and money are spent on trying to solve problems that silos have created.

FIGURE 1: CURRENT APPROACH. AT THE AGGREGATE LEVEL, FINANCIAL INSTITUTIONS ARE DEALING WITH MULTIPLE SILOS.



Why silos create significant limitations for the effective management of financial crime risks

Internal suspicions are escalated to specialist teams due to the sensitivity and complexity of the information. The treatment of internal escalations is driven by factors within the internal and external environment, both of which can have negative impacts on the business.

Internal Drivers

Systems infrastructure: Large-scale organisations are often subject to multiple legacy systems and different data sets that are incompatible with one another. Without a system-agnostic common platform, financial crime intelligence sharing across the organisation is difficult. In a survey of financial crime and Anti-Money Laundering (AML) compliance professionals, 87% cited disparate systems that do not interoperate as a significant challenge[3].

Operational process: Global Policies and Standards are underpinned by operational procedures that are constructed according to the needs of the local department and business line. This segmented approach to financial crime investigations can be self-defeating. These inconsistencies can lead to criminals exploiting jurisdictions or business lines with perceived weaker financial crime controls, undermining the reputation of the institution.

Team bias: The investigation is undertaken often with no reference to the existing intelligence within the bank. 86% of polled executives and employees blame a lack of collaboration or bad communication for team problems and failures[4].

External Drivers

Regulatory environment: Regulation commences with international principles published by organisations such as FATF and the United Nations. The application of these principles may pass through separate continental directives, national legislation and industry guidance before it filters into organisational policy. The larger the organisation's global footprint, the more regulation it must adhere to, and the less likely it is to share that information across the business.

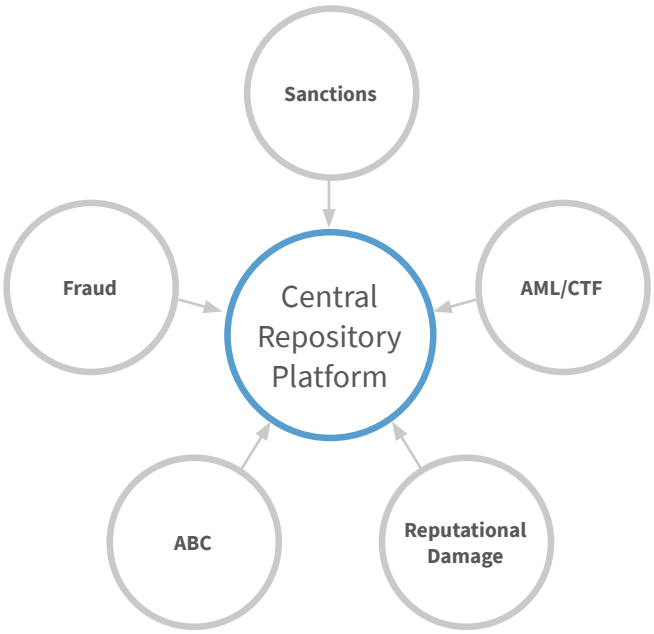
3 https://www.finextra.com/newsarticle/30631/legacy-tech-will-become-barrier-to-fighting-financial-crime---survey

4 https://www.salesforce.com/blog/2012/09/nick-stein-work-post-2.html

Data protection: Legislation can impede intelligence sharing across borders. This can result in teams working separately and not collaborating due to perceived restrictions. For example, in the context of GDPR, the CEO of the European Banking Association stated "We have the GDPR in Europe and it is a great regulation that protects the privacy of citizens. But when it leads to the protection of criminal networks, something is wrong. In my view, the GDPR gives the opportunity to do good law enforcement and exchange of information, but it's lacking."[5]

A new approach: why technology is the solution

Consolidating bank-wide financial crime intelligence should be viewed as a natural evolution rather than a revolution.



As the methods of financial crime become more complex and the cost of managing these risks continues to rise, organisations need to find an effective method to consolidate their existing intelligence to combat financial crime.

Centralised intelligence sharing platforms that autonomously identify potential commonalities between existing open and closed investigations already exist in the market. Such platforms are designed to be system-agnostic, with the ability to synthesise multiple data sources and formats, making it accessible to all departments and lines of business. This eliminates the need for financial institutions to instigate a costly IT infrastructure overhaul.

5 https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/banks-need-steer-on-data-protection-vs-money-laundering-rules-industry-bodies-57199496

"As the methods of financial crime become more complex and the cost of managing these risks continues to rise, organisations need to find an effective method to consolidate their existing intelligence to combat financial crime."

Managing data privacy remains an important issue, but one that has been solved by technology solutions by ensuring that full control over data sharing is retained by the investigation owner. Some platforms have integrated warnings and prompts to guide the user through the process of setting up collaboration on investigations and intelligence sharing. Functionality such as document sharing and the ability to create a suspicious and/or fraudulent documentation library creates an efficient mechanism to share important intelligence across multiple teams.

Unlocking value: the key benefits of a technology-driven approach

An internal cooperative approach to financial crime intelligence fosters an inclusive mentality and drives measurable value for an organisation, not only in the way it manages financial crime risks, but also financially and reputationally.

Cost and resource efficiency: Significant cost savings can be achieved by eliminating the duplication of efforts. No longer would multiple investigators be conducting the same checks on the information that has been assessed elsewhere in the organisation as they can leverage off one another. Investigation time can be reduced significantly to free-up resources for other activities through utilising pre-existing client investigative data and documentation.

Positive customer outcomes: Centralised intelligence sharing will inevitably drive a reduction in the frequency and volume of client outreach as existing information and documentation is reused.

Embracing risk: Collaboration helps to identify a holistic picture. Centralised management information can highlight problematic industry or client types to help drive business decisions and strategy. This is also important for rebalancing the portfolio and identifying new market opportunities as part of the enterprise-wide risk assessment.

Enhancing security: A centralised intelligence sharing platform and watchlist will provide a robust tool against those who seek to exploit different jurisdictions or business lines. Intelligence-led financial crime risk management will protect the organisation's reputation and reduce the risk of receiving regulatory fines.

Now is the right time to break silos

Organisations need to explore methods to integrate their financial crime intelligence. The ability to do so will foster collaboration, reduce costs, reduce unnecessary customer outreach, and protect the reputation of the organisation.

The adoption of advanced risk management systems and a culture of embracing innovation will help financial institutions to get ahead of the constantly evolving financial crime threats.

This technology already exists, so it is time to exploit the next logical, evolutionary step.

CRAIG ROBINSON
Senior Director, Digital Risk and Compliance
+44(0)20 7632 5014
craig.robinson@fticonsulting.com

LIZ JORDAN
Senior Director, Digital Science
+44(0)20 3727 1634
liz.jordan@fticonsulting.com

1035 - 06/20