COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

The importance of transaction monitoring, and the cost of getting it wrong

By Teodora Harrop, for International Compliance Association | Tue, Aug 3, 2021 1:36 PM

Transaction monitoring has evolved to the point where the emphasis is now on the requirement firms carry out ongoing monitoring of client relationships. Financial institutions have invested significantly in response, but regulators across a range of jurisdictions continue to impose significant fines against firms that fail to monitor transactions effectively.

ICA INTERNATIONAL COMPLIANCE ASSOCIATION

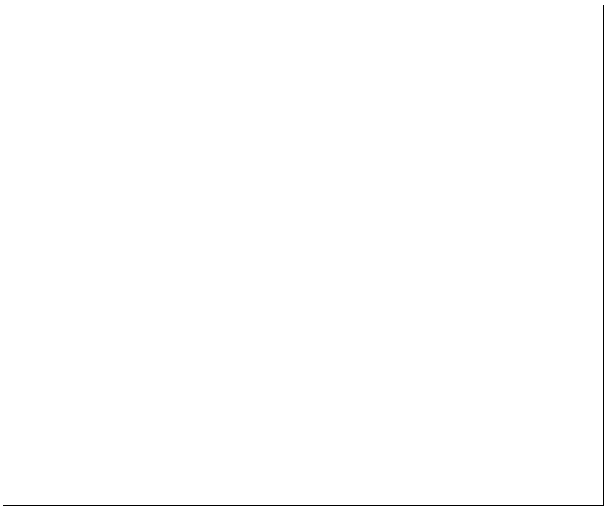
The International Compliance Association (ICA) is a professional membership and awarding body. ICA is the leading global provider of professional, certificated qualifications in anti-money laundering; governance, risk, and compliance; and financial crime prevention. ICA members are recognized globally for their commitment to best compliance practice and an enhanced professional reputation. To find out more, visit the **ICA website**.

In September 2020, AUSTRAC fined Westpac a record AUS$1.3 billion (then-U.S. $912.6 million) for **failing to properly report** an incredible 19 million cross-border transactions and carry out appropriate due diligence in relation to those payments, noting some could have been associated with human trafficking and child exploitation activities.

Similarly, in June 2020, Commerzbank was fined £37.8 million (then-U.S. $47.4 million) by the U.K. Financial Conduct Authority (FCA). One of the **issues identified by the FCA** related to failure to "address long-standing weaknesses in [the bank's] automated tool for monitoring money laundering risk on transactions for clients." Despite identifying in 2015

that 40 high-risk countries were missing and 1,110 high-risk clients had not been added, Commerzbank delayed making the required changes to the tool.

And in February, the Office of Foreign Assets Control (OFAC) fined BitPay $507,375. Despite the lower penalty, this **enforcement action** brought an interesting dimension to the concept of transaction monitoring, as one of the key issues related to BitPay's failure to include location data in its transaction monitoring program.



Though BitPay screened its direct customers (the merchants) against OFAC's sanctions list and conducted due diligence on them to ensure they were not located in sanctioned jurisdictions, it failed to screen location data it obtained about its merchants' buyers.

These fines illustrate adequate transaction monitoring can help firms evidence they are complying with legal and regulatory requirements and that an absence of effective tools can have serious ramifications.

Preventing complex crime

While the risks associated with money mules are relatively well-known, an effective transaction monitoring system might help detect other types of more sophisticated crimes.

For example, in October 2019, the U.K.'s National Crime Agency (NCA) **highlighted the risks** of Chinese underground banking (an informal value transfer system) and the practice of "daigou" (purchasing goods in a Western country on behalf of third parties in China).

Following several prosecutions, the NCA identified instances of abuse of Chinese underground banking "by utilizing cash generated from crime in the U.K. to settle separate and unconnected inward Underground Banking remittances to Chinese citizens in the U.K."

Persons involved in daigou receive "criminally derived cash directly into their U.K. bank accounts, or wire transfers from mule accounts in the name of other Chinese nationals, into which criminally derived cash has previously been 'smurfed.'"

The right blend of automatic and manual systems

When it comes to transaction monitoring, legislation is not prescriptive—financial institutions can adopt different approaches. A manual approach can be incredibly resource-intensive and is less likely to be able to adapt in response to emerging risks, but the cost of automated systems may be substantial.

In its "**Financial Crime Guide**," the FCA highlights examples of good practice, asking firms to consider how they "feed findings from monitoring back into the customer's risk profile" and reminding firms of the importance of understanding the "capabilities and limitations" of automated transaction monitoring systems.

The Monetary Authority of Singapore in 2018 **published a paper** produced by the AML/CFT Industry Partnership that highlighted the importance of ensuring compliance with legal and regulatory requirements, including data privacy:

FIs [Financial institutions] wishing to embark on analytics projects will need to have a clear understanding of the relevant regulatory considerations, particularly in respect of ever developing and evolving legal and regulatory requirements. FIs would need to evaluate any apparent inconsistencies between their proposed models and regulatory requirements, then design or adjust models in order to work within regulatory parameters. In addition to AML/CFT regulations, data privacy and protection laws are also relevant as they govern the collection, disclosure, and data, especially personal data, in the jurisdictions within which the FIs operate or have customers.

An effective transaction monitoring system might employ an automated approach but will still rely on a certain level of manual, human intervention. Individuals should:

- Document the scope of transaction monitoring, including screening of any additional information (such as IP addresses);

- Calibrate the systems and rules. Some “off-the-shelf” solutions might lack flexibility or will involve significant time and resource to be adapted to respond to emerging risks (such as the pandemic);
- Review the potential issues identified. These could relate to a range of financial crime issues, from money laundering or fraud to sanctions evasion;
- Assist financial institutions to comply with legal and regulatory requirements, including reporting of suspicious activities and transactions;
- Comply with data privacy requirements, prevent data breaches, and protect against cyber-attacks;
- Provide reporting to senior management and regulators; and
- Undertake assurance activities proportionate to scale and complexity.

Each firm will have to identify and document the correct transaction monitoring approach for its business model and strategy. Culture, education, and training are key in preventing financial crime. The ramifications of enforcement actions can be financially and reputationally damaging for firms, but failure to protect the vulnerable can have far-reaching implications for both financial institutions and society.

The International Compliance Association is a sister company to Compliance Week. Both organizations are under the umbrella of Wilmington plc.

RATE THIS RESOURCE

Select your rating

