Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Automated AML Compliance Tools Are No Silver Bullet

By **Ian Hargreaves, Ian Redfearn and Josianne El Antoury**
(February 4, 2022, 3:50 PM EST)

Ian Hargreaves

Ian Redfearn

Regulated financial institutions are increasingly using automated compliance tools, including transaction monitoring systems, as part of their anti-money laundering risk mitigation measures.

According to business data platform Statista, the AML software market is expected to increase in value to $1.77 billion worldwide in 2023, from $690 million in 2016.[1]

However, automation is no silver bullet. As the sector moves toward greater use of automated transactions monitoring systems, regulated financial services firms must take care not to become overreliant on automated approaches, which may not be fully fit for purpose.

This article discusses regulatory expectations regarding the use of AML technologies, and considers potential liability and insurance coverage implications arising from reliance on these tools, particularly when the tools are provided by third parties.

Regulatory Expectations

Authorized financial services firms are required to have systems and controls in place to mitigate the risk that they might be used to commit financial crime. Breach of this obligation can give rise to offenses under the Money Laundering, Terrorist Financing and Transfer of Funds, or (Information on the Payer) Regulations 2017, as well as regulatory action by the Financial Conduct Authority for violation of the rules set out in the FCA handbook.

For financial services firms dealing with high-volume transactions on a regular basis, automated transaction monitoring systems are crucial in analyzing transactions, identifying potentially suspicious activity, and meeting legal and regulatory obligations. Typically, such systems are configured to generate an automatic alert if certain preset conditions are satisfied — for example, if the value or frequency of transactions is out of line with previous account activity or with the account holder's known source of funds.

In turn, automatic alerts typically are reviewed manually by compliance professionals to determine

whether further action is required, such as submitting a suspicious activity report to the National Crime Agency.

However, the impact of these tools depends on how they are used in practice. Inadequate monitoring parameters and incomplete data can reduce the effectiveness of automated systems, allow suspicious transactions to occur without being flagged for review, and expose regulated financial services institutions to legal and regulatory risk.

Several recent FCA enforcement actions illustrate the potentially serious repercussions for financial services firms when these automated systems are found not to be fit for purpose.

NatWest

The FCA recently pursued against National Westminster Bank PLC its first criminal prosecution under the AML legislation that preceded the MLR 2017. The case related to NatWest's failure to properly monitor the activity of a commercial customer who deposited approximately £365 million ($494 million) with the bank over a period of about four years, including about £264 million in cash deposits.

NatWest was fined £264.8 million by the Southwark Crown Court, which reflected a significant reduction for a guilty plea. The court also issued a confiscation order and required the bank to pay the FCA's costs. In her sentencing remarks, Judge Sara Cockerill made clear that NatWest was "in no way complicit in the money laundering which took place," but the bank was "functionally vital" in the sense that money could not be effectively laundered had it not been for the bank's AML failures.

Among other things, the bank's automated transaction monitoring system incorrectly recognized some cash deposits as check deposits. Crucially, rules governing check deposits were less stringent. In addition, the rules used to automatically monitor transactions were reviewed infrequently and occasionally switched off.

HSBC

In the same week as the NatWest sentencing in December 2021, the FCA fined HSBC Bank PLC £63.9 million for breach of the AML rules that preceded the MLR 2017 over a period of eight years to 2018.

The three key deficiencies were a failure to:

- Consider whether the scenarios used to identify indicators of money laundering or terrorist financing covered relevant risks until 2014 and carry out timely risk assessments for new scenarios after 2016;

- Appropriately test and update the parameters within the systems that were used to determine whether a transaction was indicative of potentially suspicious activity; and

- Check the accuracy and completeness of the data being fed into, and contained within, monitoring systems.

The FCA did recognize, however, HSBC's commitment to its large-scale global remediation program and noted several successful enhancements to improve data quality.

While the FCA's enforcement action in these cases was brought under the legislation that preceded the MLR 2017, the actions are indicative of the FCA's continuing focus on the adequacy of AML systems and controls, even in circumstances where it cannot be established that a financial institution has actually been involved in money laundering itself.

Moreover, the successful NatWest prosecution is likely to encourage future criminal prosecutions by the FCA in appropriate cases.

Liability and Insurance Considerations

The FCA expects regulated firms that choose to use third parties to provide automated AML tools to retain ultimate responsibility for the outsourced activities.

For example, for certain types of regulated institutions that rely on third parties for the performance of critical operational functions, the FCA handbook requires that those firms take reasonable steps to avoid undue operational risks, and to undertake the outsourcing in a way that does not materially impair the quality of internal controls or the ability of the FCA to monitor the firm's compliance with its regulatory obligations.

A failure to oversee the proper maintenance of automated compliance controls provided by third parties therefore may result in FCA action. The Information Commissioner's Office will also have a keen interest in ensuring the automated tools comply with the General Data Protection Regulation.

It is also important that the relevant software is properly updated and continues to meet manufacturer standards, not least because this could give rise to criminal exploitation by cybercriminals.

Where the provision or implementation of automated AML tools is outsourced, proper allocation of risks in the outsourcing agreement will be key.

Financial institutions should take care to check their agreements with the relevant third parties to understand whether there is any potential insurance coverage from the third parties' insurers if products are not fit for purpose or if the third parties mishandle customer data.

Policyholders or their coverage counsel should also consider other current lines of insurance to assess potential paths to coverage in the event of consequential losses arising out of the use of automated AML compliance tools — for example, customer data loss or business interruption loss resulting from deficient tools.

In the U.K. particularly, steps have been taken to eliminate what is referred to in the market as silent cyber — that is, potential coverage for cyber-related risks in property and liability insurance policies that do not explicitly include or exclude cyber risks.

Nonetheless, other traditional property and casualty insurance policies, including general liability, property damage and business interruption policies should still be analyzed for any potential coverage in circumstances where deficient automated tools give rise to losses.

In the context of ransomware cover under cyberinsurance policies, we are already seeing restrictive endorsements being introduced by major cyber insurers, which narrows cover by adopting a sliding

scale of risk-sharing with the insured, when the insured fails to update a known software vulnerability.

This means that the longer an insured has failed to update software that was exploited in a cyber incident, the lower the insurer's limit of liability and the higher the insured's share of the loss arising from the incident.

In circumstances where the money laundering reporting officer or directors are being investigated for poor oversight of AML controls, directors and officers liability insurance would usually cover the costs of responding to a formal investigation, but may not always cover pre-investigation work — depending on the policy wording.

FCA civil and criminal fines will be uninsurable as this is expressly stated in the FCA handbook. However, the position is less clear for GDPR fines and will ultimately be fact-specific and depend on an assessment of the public interest and the policy wording.

Ian Hargreaves is a partner, Ian Redfearn is special counsel and Josianne El Antoury is an associate at Covington & Burling LLP.

[1] https://www.statista.com/statistics/864814/worldwide-anti-money-laundering-software-market-size/.