AASG
Accountancy AML Supervisors' Group

Risks and vulnerabilities for money laundering through capital markets

Extract from NCA Amber ALERT of July 2020 (References 0612 - NECC)

Overview

The purpose of the alert is to outline some of the main money laundering risks and vulnerabilities within the global capital markets.

Background

Money Laundering Through Markets (MLTM) involves the abuse of capital markets products (shares, derivatives, bonds and other instruments) and transactions to move or obscure the origin, destination or ownership of already existing illicit funds. It doesn't include illegal activities that generate criminal funds within the capital markets eg, insider dealing or market abuse.

MLTM risk indicators

The risk indicators relate to outcomes that products facilitate, rather than attributes of a particular product. Individually, the outcomes may be legitimate but risk is highest when multiple outcomes are combined.

- **Lack of economic rationale** – consider the rationale for why the client wants to trade – a lack of economic rationale may indicate risk eg disinterest in profit or makes little profit or loss.
- **Facilitates currency change** – moving monies between currencies may present risk when combined with other risk factors. Higher risk exists where the client moves between currencies by trading near-simultaneously in close-related jurisdictions (mirror-trading).
- **Facilitates jurisdiction change -** particularly with high-risk jurisdictions. This would include jurisdiction switching where the client and broker are in different jurisdictions or where the client sets up an account in one jurisdiction but trades from another.
- **Value/volume limit avoidance** – The client may know limits for the market participant and avoids reaching those limits to avoid detection.
- **Higher-risk periods or external trigger events** – this may include an increase in trade at certain times eg, tax year end, to meet end-of-year performance criteria, or a change in legislation (eg, sanctions regimes).
- **Third party payments (TPP)** – payments using third parties present higher risk as the third party may obscure ownership, may not be onboarded and may not always be effectively monitored.
- **Outliers** – where a client is not acting in line with its peers. This will also include where a client offers more margin or collateral than required (overfunding).
- **Unexpected, or sudden change in, business activity** – consider: dormant accounts; unexpected behaviour changes in activity; trading a wide variety of unrelated instruments; volume/value of trade does not reflect size/scale of client.

MLTM vulnerabilities

It is important to be aware of the vulnerabilities of capital markets, which may create obstacles from effectively detecting and mitigating MLTM risks. It is unlikely that one entity will have full visibility over the end-to-end transaction cycle, which may impede the understanding of the overall economic rationale. Furthermore, AML monitoring tools have not been effective to date in detecting suspicious MLTM activity – particularly as they tend to identify suspicious trades rather than the illicit funds behind them. Finally, CDD procedures have not always been effective in identifying the MLTM risk indicators.

Suspicious Activity Reporting [SARs]

If you know or suspect ML or TF activity you should make a SAR and include the alert reference **0612-NECC** within the text *in addition* to the ongoing use of the Glossary of Terms. Guidance on reporting is available at: www.nationalcrimeagency.gov.uk

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer