Protiviti - Unchartered territory: Addressing Russian sanctions evasion

Individuals and entities will often take steps to avoid the impact of sanctions. Below, Protiviti explores sanctions evasion tactics and what financial institutions can do to mitigate evasion risk.

This article is based on the recent Protiviti webinar series Unchartered Territory: Managing the Risk of Russian Sanctions held in the US, the UK and the EU.

Sanctions evasion tactics are well established and remain a focal point for financial institutions as additional Russian sanctions unfold. They can take many forms, including leveraging local laws to execute transactions anonymously, employing front and shell companies to obfuscate transactions, laundering money, and creating complex ownership structures or transferring control of assets.

Their widespread use has "implications for firms understanding their customers", according to Stefanie Dohman, associate director at Protiviti UK.

Authorities are on high alert for cases of evasion. The US Department of the Treasury's Office of Foreign Assets Control (OFAC), in coordination with the EU, the UK and Japan, has been targeting Russian sanctions evasion networks utilizing front and shell companies in multiple countries to illegally procure western technology for the benefit of the Russian military and intelligence agencies.

An emerging channel for sanctions evasion is blockchain, as the technology's mechanism for tracking transactions digitally may be undermined by crypto exchanges that conspire to conceal the sources of customers' funds.

'It's therefore important for financial firms to keep a close eye on the phases of exchange between crypto and fiat currencies, and undertake due diligence on the parties involved, before entering the blockchain', says Jackie Sanz, managing director at Protiviti in Toronto.

Enlisting the help of the three lines of defence

All three lines of defence have a role to play in identifying and preventing sanctions evasion.

The first line of defence should be trained to conduct enhanced due diligence (EDD), understand ultimate beneficial owners (UBO) and perform link analysis. Name screening and transaction filtering may help avoid false positives and potential misjudgements due to outdated or incomplete Know Your Customer (KYC) data.

'The interaction between KYC teams and sanctions and embargo units should also be enhanced', says Cornelia Tomczak, director at Protiviti in Frankfurt. 'This goes beyond regulatory requirements to the backgrounds of customers, business partners and vendors alongside the assurance of products, including trade finance, syndicated loans, and credit cards. Collaboration with regulatory bodies will also be important'.

The second line of defence should identify and understand the nuances of sanctions regulations and how they may impact client relationships. Compliance may want to review, update and strengthen policies, procedures and training.

The third line of defence should focus on the skills needed to perform testing procedures and understanding sanctions evasion tactics. In the US, the Financial Crimes Enforcement Network (FinCEN) has issued a list of red flag indicators.

A marathon, not a sprint

Financial institutions should think of sanctions evasion risk management as a marathon and seek to develop thoughtful, comprehensive programmes with repeatable, scalable processes that can be tested.

Sanctions will continue to evolve and be used by governments to advance political and diplomatic agendas. Through more rigorous vetting, financial institutions can better position themselves to detect and thwart efforts to evade them.

For more information on sanctions compliance, please contact Bernadine Reese, managing director at Protiviti UK at bernadine.reese@protiviti.co.uk.