WEAPONIZING THE FINANCIAL SYSTEM BRINGS MONEY LAUNDERING RISKS

Authored by: Nathan Shaheen - Bennett Jones

In response to Russia's invasion of Ukraine, Western countries and their allies have weaponized the global financial system to target the world-wide assets of Russia and its wealthy oligarchs. One of the consequences is likely to be enhanced money laundering risks, not just for traditional financial institutions, but for businesses in a wide range of industries worldwide. Such businesses would be well-served to take the steps required to understand the rapidly-evolving landscape and to mitigate the risks of facilitating money laundering and related financial misconduct.

The Weaponization of the Financial System

Russia's invasion of Ukraine is the largest conventional military attack in Europe since the Second World War. While the Ukrainian military and armed civilians have met force with force, Western countries and their allies have thus far steadfastly maintained that their troops will not directly engage in armed conflict. Instead, those countries have primarily responded to Russian aggression by utilizing a wide array of financial tools against Russia and its oligarchs, and against Russian leader Vladimir Putin himself.

The financial tools being utilized by Western countries and their allies are increasingly a strategy of first resort against both state and non-state actors. The September 11th attacks led to the immediate introduction of laws aimed at better intercepting the flows of illicit funds to terrorists. Iran remains subject to sanctions in response to its nuclear programs. The Canadian government recently, and controversially, responded to the so-called "Freedom Convoy" protests against Covid-19 mandates by freezing the bank accounts and certain other assets of the protestors.

The financial tools being utilized in response to Russia's invasion are nonetheless notable in their breadth and seriousness. In addition to prohibitions on importations of key Russian resources such as coal, Western countries have joined together in banning transactions with the Russian central bank, and banning key Russian banks from the international payment system (SWIFT). On April 6th, U.S. President Joe Biden issued an Executive Order [1] prohibiting U.S. citizens from making new investment in, or providing various services to, Russia. Sanctions have also been leveled against Putin, his adult daughters and an ever expanding list of Russian lawmakers and oligarchs, whose foreign assets have been targeted and in some cases seized

The nature and extent of the financial tools being deployed by Western countries and their allies have been understandable described as "weaponizing the financial and payments system [2]."

1 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/04/06/prohibiting-new-investment-in-and-certain-services-to-the-russian-federation-in-response-to-continued-russian-federation-aggression/

2 https://www.brookings.edu/opinions/economic-warfare-is-hurting-russia-but-its-risky-for-the-us-too/

The Consequences of Financial Warfare

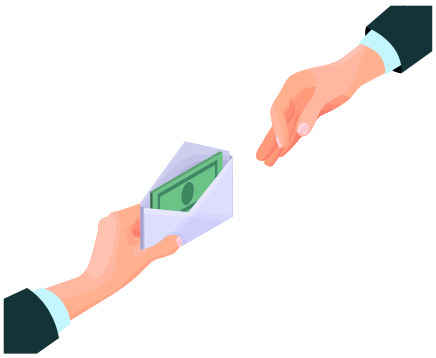
The use of financial tools in response to Russian aggression will naturally be felt most directly by Russians. This is true of average citizens living in Russia, but equally of the oligarchs who, whether physically within Russian or elsewhere, have long enjoyed their vast holdings of significant foreign assets. The impacted sums are staggering.

A 2018 study [3] estimates that, by 2015, the hidden assets of wealthy Russians amounted to 85% of Russia's GDP.

The impacts of the financial tools being employed by Western countries will also be felt more broadly. In addition to the broader economic fallout, there are obvious implications for businesses directly engaged in Russia or with Russian counterparts. Such activity has been increasingly restricted, whether as a matter of law, logistics or public relations. Such restrictions are likely to remain and even expand as the Russian aggression continues.

Notably, the risks are also likely to spread beyond those businesses directly engaged with Russia. The restrictions placed on the significant foreign assets of Russian oligarchs create the strong possibility that oligarchs will respond by engaging in creative and increasingly complex tactics in an attempt to maintain access to their global wealth and the lifestyles such wealth affords. In addition to constituting illegal sanctions evasion [4], such tactics would constitute money laundering or related financial misconduct under the laws of jurisdictions around the world, and may lead the price for laundering funds higher as demand for, and sophistication of, money laundering practices reach new heights.

In turn, the risks of inadvertently facilitating money laundering or similar financial misconduct is likely to be heightened, not just for traditional financial institutions, but for businesses in a variety of industries worldwide. For example, various forms of corporate financings, investments, capital-intensive projects or other transactions could inadvertently shelter the movement or use of assets subject to sanctions or similar restrictions. Consistent with widespread reports[5], such risks may be most acute for businesses engaged in the emerging cryptocurrency sector, although many business engaged in the movement or investment of funds could conceivably face similar issues, particularly where the funds may have been subject to underlying failures of due diligence or inadequate sanction adherence.



How Businesses Should Respond

In the face of the increased risks of facilitating money laundering or similar financial misconduct resulting from pressures arising from Russia's ongoing aggression, businesses in would be well served to ensure they are taking the steps required to understand and respond to the rapidly-evolving landscape in order to mitigate those risks.

In this context, risk mitigation includes implementing or maintaining sufficiently robust policies and procedures to respond to the heightened risks of money laundering, including with reference to the emerging global standards in respect of the transaction of cryptocurrencies [6]. Such standards are consistent with the growing attention being paid by legislators, including President Biden [7], to the potential for government intervention aimed at stemming the misuse of cryptocurrencies as a matter of financial stability and national security. Other countries will surely soon follow suit.

Such policies and procedures must then be applied in a manner that keeps up-to-date with and understands the rapidly-evolving landscape, and then the associated risks into account when undertaking transactional due diligence and otherwise evaluating appropriate business relationships.

This is particularly true where counterparties to those relationships are in higher risk industries or conduct business in jurisdictions where sanctions or other financial controls may not be sufficiently robust.

These forms of responses are relevant not only to mitigating the particular money laundering risks arising from the ongoing Russian aggression, but equally to a world where weaponizing the financial and payments system appears likely to remain a tool of first resort used by Western countries and their allies.

3 https://gabriel-zucman.eu/files/NPZ2018.pdf#page=17
4 https://www.justice.gov/opa/pr/russian-oligarch-charged-violating-us-sanctions
5 https://www.reuters.com/business/exclusive-russians-liquidating-crypto-uae-seek-safe-havens-2022-03-11/
6 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html
7 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/