

March 7, 2022: [FinCEN issues Alert on Potential Russian Sanctions Evasion Efforts](#)

OVERVIEW

The Financial Crimes Enforcement Network (FinCEN) issued an Alert [FIN-2022-Alert001] to financial institutions, highlighting the potential for sanctioned individuals and entities within Russia and Belarus to attempt to evade expansive sanctions and other measures implemented in connection with the Russian Federation's ongoing, unprovoked invasion of Ukraine. The alert provides example red flags to assist in identifying suspected sanctions evasion activity.

All financial institutions—including those with visibility into cryptocurrency or convertible virtual currency (CVC) flows, such as CVC exchangers and administrators—should identify and report suspicious activity associated with potential sanctions evasion quickly and conduct appropriate, risk-based customer due diligence or enhanced due diligence where required. Financial institutions are also encouraged to make full use of the information sharing authorities provided by Section 314(b) of the USA PATRIOT Act.

KEY INSIGHTS

- The unprecedented economic pressure imposed by the United States and key U.S. partners will not have their intended impact if financial institutions are not monitoring for red flags related to potential sanctions evasion activity associated with Russia and Belarus.
- Visibility into CVC flows by CVC exchangers and administrators is especially important and those MSBs must identify and report quickly any suspicious activity associated with potential sanctions evasion.
- Given the diverse range of sanctioned individuals, entities and financial institutions, all financial institutions have an immediate need to assess their potential exposure to sanctioned persons, assets and financial activity and take swift remedial action to address identified instances of sanctions exposure.
- On March 12, SWIFT will disconnect seven Russian banks from their network, which will require all financial institutions to address potential disruptions in payment flows and payment operations.

HOW WE CAN HELP

We understand that sanctions related to the Russia / Ukraine conflict are coming out quickly and changing almost daily. It is difficult to keep up with these new requirements while operating your daily processes. Exiger can help support “Run the Bank” processes while you strategically tackle these new sanctions. We can also help you identify and monitor your sanctions exposure, especially any activity related to sanctions evasion, by helping with transaction monitoring, SAR drafting and/or database lookbacks.

- ⇒ Read Exiger CEO's, Michael Cherkasky, [statement](#) on Exiger's stance on Russia's recent actions
- ⇒ For information and helpful resources regarding the ongoing crisis and how we can help, please reference our [Russia-Ukraine Conflict Knowledge Hub](#)
- ⇒ [Double your donation](#): If you'd like to contribute to the emergency response efforts in Ukraine, Exiger is proud to be matching up to \$25,000

ABOUT EXIGER

Exiger is revolutionizing the way banks, corporations, and governments manage risk through its combination of practical expertise, award-winning technology, and process excellence. In recognition of the growing volume and complexity of data and regulation, Exiger is committed to creating a more sustainable compliance environment through its holistic and innovative approach to problem solving. Powered by DDIQ and Insight 3PM, Exiger takes an analytics-led, technology-enabled approach to everything we do.

For more information, contact:

Tara Loftus

Managing Director, Exiger Advisory Solutions

tloftus@exiger.com

Chris Andre

Managing Director, Exiger Advisory Solutions

candre@exiger.com