COMPLIANCE CIRCULAR	**5/2022 [CC 5_2022]**
To:	**ALL MEMBERS AND COMPLIANCE OFFICERS OF THE INSTITUTE**
Date:	**10 March 2022**
Subject:	**Financial Crimes Enforcement Network of USA alert in relation to Potential Russian Sanctions Evasion Attempts**

ICPAC wishes to notify its Members of the alert issued by Financial Crimes Enforcement Network of USA (FinCEN) in relation to Potential Russian Sanctions Evasion Attempts.

The document, among other information, provides a very useful list of red flags to assist in identifying potential sanctions evasion activity. The red flags cover both evasion attempts through the use of the financial system as well as virtual currencies.

Please see below a list of the relevant Red Flags:

1. Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.

2. Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration.

3. Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.

4. Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale.

5. Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations.

6. Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

7. Non-routine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity over the prior 12 months. For example, the Central Bank of the Russian Federation may seek to use import or export companies to engage in foreign exchange transactions on its behalf and to obfuscate its involvement.

8. A customer's transactions are initiated from or sent to the following types of Internet Protocol (IP) addresses: non-trusted sources; locations in Russia, Belarus, FATF-identified jurisdictions with AML/CFT/CP deficiencies, and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious.

9. A customer's transactions are connected to Virtual Currency addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List.

10. A customer uses a Virtual Currency exchanger or foreign-located MSB in a high-risk jurisdiction with AML/CFT/CP deficiencies, particularly for Virtual Currency entities and activities, including inadequate "know-your-customer" or customer due diligence measures.

ICPAC Members are urged to take the above red flags into consideration, remain vigilant and incorporate them into their due diligence measures.

To access the full document, please follow the link