



# Regulatory Alert

## Regulatory Insights



March 2022

### U.S. actions to Russia-Ukraine war: Expanded regulatory attentions

*Financial services companies are facing rapid and iterative OFAC sanctions and Administration executive orders. Regulators will expect companies to comply with the new requirements as well as monitor and mitigate compliance risks directly and via counterparties, third parties, etc. In addition, regulators are signaling expanded attention to financial crimes, cyber security, and crypto and digital assets. Regulatory expectations in these areas are evolving though all are tied to the Administration's whole-of-government national security initiatives and as such are already subject to heightened attention. Notably, both Treasury and the Federal Reserve Board have denoted increased attention to crypto and digital assets.*

The U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) released [new guidance](#) on March 2, 2022 intended to strengthen compliance with the previously announced sanctions directed at Russian financial institutions and other designated entities and individuals (see *KPMG Regulatory Alert*, [here](#)). The new guidance is [detailed](#) in Frequently Asked Questions and General Licenses. It was quickly followed by an additional [release](#) outlining new sanctions against Russian individuals, entities, and assets.

#### Potential areas of regulatory focus

OFAC released a [Framework for OFAC Compliance Commitments](#) (Framework) in 2019 to outline essential components of a sanctions compliance program. The Framework applies to organizations subject to U.S. jurisdiction, and foreign entities operating in or with the U.S., U.S. persons, or using U.S.-origin goods and services. Areas highlighted by the guidance include those called out below. (See *KPMG Regulatory Alert*, [here](#)).

Under this Framework, a sanctions compliance program should include multiple areas of coverage, including:

- Adoption of a formal compliance program that includes separation of duties and control processes; protocols for identifying, interdicting, escalating, resolving and reporting red flag issues; adequate and skilled resources (human capital, expertise, IT capabilities) with ongoing training and communications
- Identification and verification of an entity's beneficial ownership as well as its geographic location, counterparties, and transactions (customer due diligence); sanctions compliance also requires identification of related entities that would trigger the 50 Percent Rule. (FinCEN issued a proposed rule in December 2021 that would implement beneficial ownership information reporting requirements as required by the Corporate Transparency Act – see *KPMG Regulatory Alert*, [here](#).)
- Periodic testing and auditing of screens/filters and systems to ensure consistency and accuracy, as well as updates based on changes to risk assessment factors (e.g., clients, customers,



products, services, supply chain, intermediaries, counterparties, transactions, geographic locations)

- Oversight of third parties, commensurate with the risk profile/complexity of the third party relationship, including i) periodic risk assessments (to ensure the third party has sufficient expertise, processes, and controls to maintain the necessary licenses to enable the financial services company to remain compliant with domestic and international laws and regulations, as appropriate, and ii) contract provisions that clearly and thoroughly document the responsibilities of the company and the third party, restrictions of activities/transactions, and management of conflicts between the U.S. and foreign country requirements. (Note, key areas of jurisdictional differentiation include data privacy, information security, Bank Secrecy Act/anti-money laundering, sanctions, and fiduciary requirements.)
- Continuous improvement, testing, and review, with immediate remediation for identified weakness and updates for lessons learned from the company's own experience and the experience of other companies facing similar risks.

**Crypto and digital assets.** The imposition of sanctions on Russia has raised concerns about the use of crypto and digital assets as a payments systems alternative that could undermine the efficacy of the sanctions regime. Members of Congress have [asked](#) OFAC to explain how it intends to enforce sanctions compliance guidance for the cryptocurrency industry. Separate, but related regulatory responses include statements from:

- Treasury Chair Yellen, who said\* that cryptocurrencies are “a channel to be watched,”

adding that Treasury “will continue to look at how the sanctions work and evaluate whether or not there are leakages, and we have the possibility to address them.”

- Federal Reserve Board Chair Powell, who stated\*\* in testimony before the House Financial Services Committee that the concerns about whether cryptocurrencies could be used to bypass sanctions “underscores the need for congressional action on digital finance including cryptocurrencies” to establish the kind of regulatory framework that is “needed.”

\* “Yellen Monitoring Russian Efforts to Evade Sanctions with Cryptocurrency, Other Means,” [wsj.com](#), March 2, 2022

\*\* “Monetary Policy and the State of the Economy,” U.S. House Financial Services Committee hearing, March 2, 2022

**Please refer to:**

- [Point of View](#) | Key Ten Regulatory Challenges of 2022 covering [Crypto and Digital Assets](#); [Cyber and Data](#); and [Fraud and Financial Crimes](#)
- [Regulatory Alert](#) | Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (DOJ)
- [Regulatory Alert](#) | Updated DOJ Guidance
- [Regulatory Alert](#) | OFAC Framework for Sanctions Compliance Programs

**For additional information,** please contact [Amy Matsuo](#), [Steve Brotherton](#), or [Tom Keegan](#).

## Contact the author:



**Amy Matsuo**  
Principal and Leader  
Regulatory and ESG Insights  
[amatsuo@kpmg.com](mailto:amatsuo@kpmg.com)

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



**Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.**

All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.