



You, Sanctions & Ince

An overview

Julian Clark, Global Senior Partner

Peter McNamee, Partner

Akshay Misra, Senior Associate

May 2022

Current sanctions

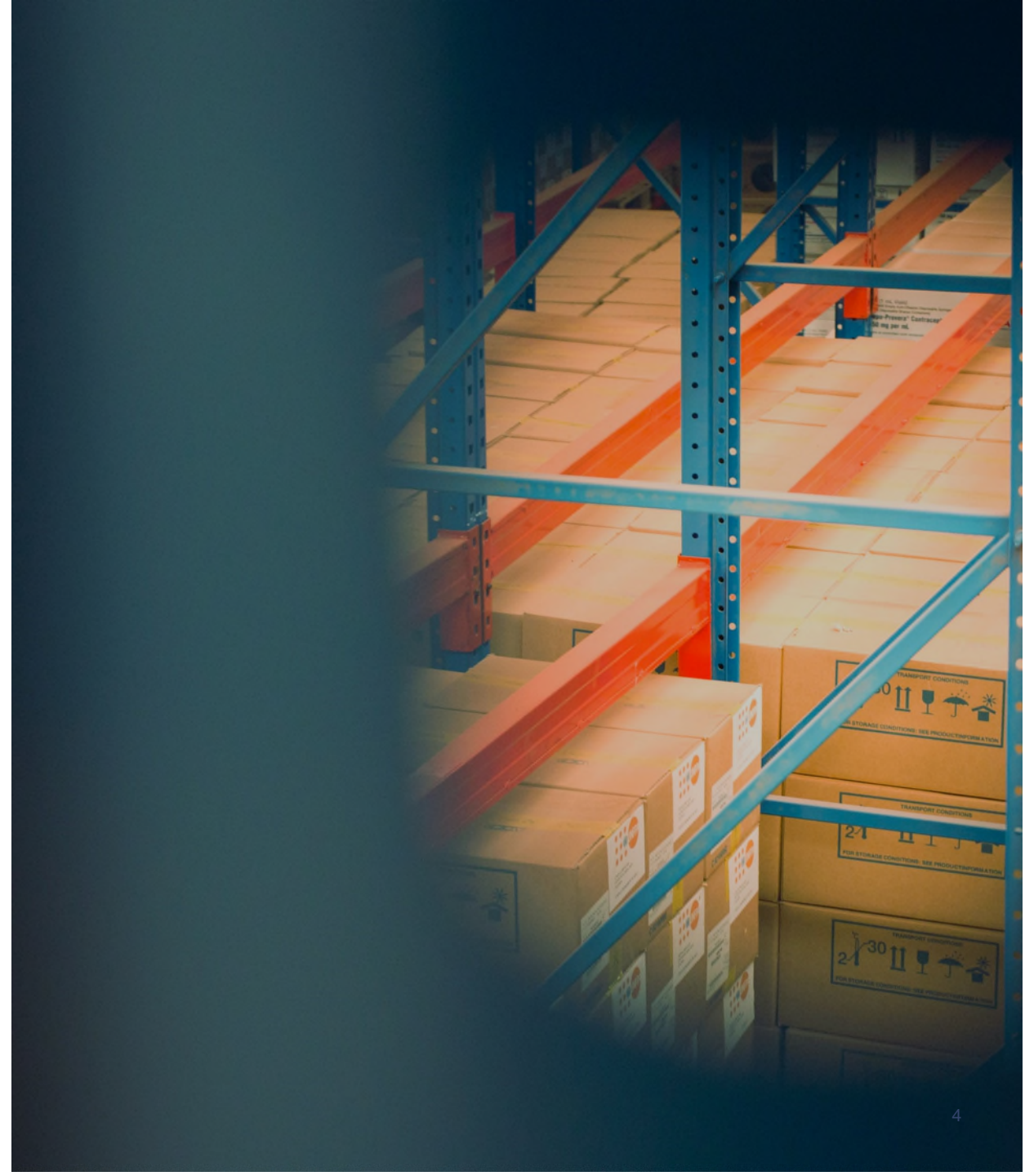
- EU sanctions operate in 33 countries.
- UNSC sanctions consolidated list includes 700 individuals and 253 entities.
- UK regimes impose sanctions on 24 countries.
- OFAC publishes lists of individuals, institutions and countries that threaten national security on a Specially Designated Nationals (SDN) list.
- There are further sanctions in place internationally in relation to cyber-attacks, the use of chemical weapons, human rights violations and abuses and Terrorism.
- Sanctions have taken several different forms: economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions.
- UN sanctions list entities and persons in North Korea, Somalia, Sudan, Mali, Libya, Yemen Afghanistan and terror outfits such as ISIL and Al- Qaeda.
- The EU sanctions list includes sanctions and restrictive measures imposed with respect to the Taliban in Afghanistan, and entities and persons in Myanmar, Nicaragua and even Turkey in view of unauthorised drilling activities in the Eastern Mediterranean.
- Currently, OFAC has imposed sanctions on entities and persons in Belarus, Burma, Cote D'Ivoire (Ivory Coast), Cuba, Democratic Republic of Congo, Iran, Iraq, Liberia, North Korea, Sudan, Syria, Venezuela, Zimbabwe.
- OFSI regimes are imposed on 24 countries including Venezuela and the Lebanon.
- The EU, OFAC and OFSI have imposed sanctions on entities and persons in Russia.

Sanctions on Russia

- The OFSI, OFAC the EU and the UN have imposed sectoral measures across finance, trade and transport on Russia following the invasion of Ukraine. In finance in the UK there has been a ban of all Russian state and private companies from capital markets.
- There are strong and increasing restrictions on central banks and their subsidiaries. Freezes of the assets of 10 key banks and sovereign wealth funds.
- The UK was the first country to ban Russian flagged flights and all Russian shipping to the UK. Furthermore, it has Sanctioned over a thousand individual entities and their subsidiaries, includes 69 oligarchs and elites.
- Each organisation is increasing sanctions as the invasion of Ukraine continues.
- In recent days, the US government has accused Russia of holding the world food supply hostage, as developing countries face famine due to lack of supplies (Russia and Ukraine produce 30% of global wheat supply and 69% of sunflower oil).
- Russia has been clear that until the sanctions imposed on it internationally begin to be lifted it will not be releasing vital grain shipments to the global community.
- Though crippling the Russian economy, oil and gas exports continue to support Russian markets.

Self – sanctions

- More than **1,000 international companies** have either suspended trading in Russia or withdrawn altogether – including **Coca – Cola, Starbucks** and **McDonalds**.
- **Nestle** has withdrawn some of its brands but will continue to sell “essential food”.
- **Ikea** will continue to operate its major chain of shopping centres, Mega, to ensure its customers have access to essentials. **Mondelez, Procter & Gamble** and **Unilever** have halted investments in Russia but will continue to provide “essentials”.
- **Maersk** halts operations in Russia. Similar bans announced by **MSC** and **CMA CGM**.



Cyber-attacks and sanctions

- Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response may risk violating sanctions.
- OFAC, OFSI the UNSC and the EU have and will continue to impose sanctions (often financial restrictions and travel bans) on ‘cyber actors’, prohibiting persons from engaging in transactions, directly or indirectly with individuals or entities (“persons”) who are listed unless authorised or expressly exempted by statute.
- OFAC emphasises that violation of sanctions is a strict liability offence. It lists mitigating factors and practices in the Cybersecurity and Infrastructures Security Agency’s September 2020 Ransomware Guide (“CISA Ransomware Guide”).

Cyber-attacks and sanctions (cont.)

These include steps to:

- Maintain offline backups of data;
- Develop incident response plans;
- Institute cybersecurity training;
- Regularly update antivirus and anti-malware software; and
- Employ authentication protocols.

In addition to the CISA Ransomware Guides, OFAC recommended that companies review the National Institute of Technology (“NIST”) and Cybersecurity Maturity Model Certification (“CMMC”) standards for additional insights and program improvements.

OFAC emphasized the importance of cooperation with law enforcement in response to a ransomware attack.

Thank you, in any case

Julian Clark

Global Senior Partner
D +44 (0) 2038 237 646
M +44 (0) 7900 167 486
E JulianClark@incedg.com

Office

Ince Gordon Dadds LLP
Aldgate Tower, 2 Lemn Street
London E1 8QN
DX 1070 London City
T +44 (0) 20 7481 0010
F +44 (0) 20 7481 4968
info@incedg.com