

JENNER & BLOCK

CLE RELAY

Global Enforcement Trends and
Emerging Risks in Sanctions, Export
Controls, and Supply Chains



US, UK, and EU Trade Regulatory Regimes

JENNER & BLOCK

US Economic Sanctions

Complex regulations with varying restrictions and obligations

Economic embargoes

Extensive country-based sanctions



Additional country-based sanctions

e.g., Afghanistan, Balkans, Burma, Lebanon, Nicaragua

Activity-based sanctions

e.g., narcotrafficking, terrorism, nuclear proliferation, corruption

US investment sanctions

Restrict US investments in Chinese Military-Industrial Complex companies

US Export Controls: What Do They Cover?

- **Overview:** Restrict the export, reexport (from a third country), or transfer (in-country) of goods, software, and technology that is “subject to the EAR” (Export Administration Regulations)
 - International Traffic in Arms Regulations (“ITAR”) is a separate regime for defense articles and services
- **What is the item and does it have a “dual use”?**
 - “Subject to the EAR” defined *broadly* to include goods, software, and technology
 1. made in the US,
 2. transiting via the US,
 3. made abroad containing certain amounts of US content, and
 4. made abroad based on certain US designs
 - “Technology” defined as *any tangible or intangible information* necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of goods, software, or technology
 - Examples: written/verbal communication, blueprints, photos, diagrams, models, design files, manuals)

US Export Controls: Where Can Items Go?

- **What country is it going to?**
 - Example: Canada vs. China
- **Who is the end-user?**
 - Example: private sector hospital vs. foreign military bio lab
 - Whether the end user on a restricted parties list
 - Entity List
 - Denied Parties List
 - Unverified List
 - Military End-User List
- **What is the end-use?**
 - Civil vs. military applications of “dual use” items
 - Military end uses



Additional US Trade and Investment Regulations

- Information Communications Technology and Services (“ICTS”) regulations
- Imports, tariffs, and customs
- Forced labor protections
- Committee on Foreign Investment in the United States
- Outbound investment restrictions



UK and EU Financial Sanctions

- Country-based sanctions
 - e.g., Russia, Syria, Belarus, Libya, Sudan, Iran, North Korea
- Activity-based sanctions
 - e.g., terrorism, human rights, corruption
- Asset-freeze restrictions
- Investment restrictions
- Trust services restrictions
- UK: Office of Financial Sanctions Implementation (OFSI) responsible for enforcement
- EU: Member states have “competent authorities” responsible for the administration/enforcement of sanctions

UK and EU Trade Sanctions and Export Controls

- Trade sanctions
 - Imports and exports restrictions
 - e.g. to and from targeted countries, for the benefit of specified persons
 - Professional services bans
 - Sanctions in relation to Russia limit the provision of professional services to Russians
 - Professional services include legal advisory, accounting, advertising, architectural, auditing, business and management consulting, engineering, IT consultancy and design, and public relations services
- Export controls
 - Governing the movement of dual-use goods and other sensitive goods
- UK: the Department for Business and Trade (DBT) has overall responsibility for trade sanctions
- EU: member states have “competent authorities” responsible for the administration of trade sanctions



Additional UK/EU Trade and Investment Regulations

UK

- **Modern Slavery Act:** requires companies to publish an annual statement setting out the steps they take to prevent modern slavery in their businesses and their supply chains.
- **Environment Act:** once secondary legislation is passed, the provisions will prohibit illegally produced forest risk commodities (include timber products) and will require businesses to establish and implement a due diligence system for such commodities
- **National Security and Investment Act:** gives the government powers to scrutinize and intervene in business transactions, such as takeovers, to protect national security, while providing businesses and investors with the certainty and transparency they need to do business in the UK
- **UK GDPR:** similar to the EU GDPR (right)

EU

- **Corporate Sustainability Due Diligence Directive:** imposes due diligence requirements and standards to assess climate change, the environment, and human rights impact posed by upstream and downstream supply chain
- **EU Forced Labour Regulation:** prohibits the sale of products made with forced labour on the EU market
- **Other industry specific regulations relating to supply chains:** EU Batteries Regulation, EU Deforestation Regulation, Conflict Mineral Regulation
- **Screening of Foreign Direct Investment Regulation:** equips the EU with a framework of a common criteria to identify risks related to the acquisition or control of strategic assets which threaten security or public order
- **General Data Protection Regulation (GDPR):** imposes obligations on organizations anywhere that target or collect data related to people in the EU

US, UK, and EU Trade Regulatory and Enforcement Trends

JENNER & BLOCK

US Trade Risks and Enforcement Trends

- More multilateral cooperation and information-sharing
 - G7 Russian asset seizure agreement
 - OFAC secondments to allies' finance ministries
- Increased interagency cooperation
 - Departments of Commerce, Treasury, and Justice “Tri-Seal” Compliance Notes on trade compliance, shipping, diversion, and disclosures
 - DOJ-BIS Disruptive Technology Strike Force
- Greater focus on export controls/sanctions by Department of Justice
 - Reorganization of NSD
 - Strategy for Countering Nation-State Threats
 - DOJ Task Force KleptoCapture

*“[S]anctions are the new FCPA. And across the department and indeed across the globe, we are handling corporate investigations that involve sanctions evasion — in **industries as varied as transportation, fin tech, banking, defense and agriculture**. And to address the increasing intersection of corporate crime and national security, the department is today announcing **significant restructuring and resource commitments within the National Security Division.**”*

*— Lisa Monaco,
Deputy Attorney General*

US Trade Risks and Enforcement Trends

- **Task Force KleptoCapture:** Recent charges, arrests, and forfeiture proceedings announcement
 - *United States v. Kostin et al.*, 1:24-cr-91-GHW (SDNY)
 - *United States v. Kurchenko*, 6:24-cr-00049 (M.D. Fl.)
 - *United States v. Feliks Medvedev*, 1:22-cr-184 and *United States v. Chubarov*, 1:24-cr-00053 (both N.D. Ga.)
 - *United States v. Osipov*, 1:22-cr-00369 (D.D.C.)
 - *United States v. Viktor Perevalov*, 24-cv-20687 (S.D. Fl.)
- **Disruptive Technology Strike Force**
 - *United States v. Kahn*, 23-mj-1133 (EDNY)
- **Agency Enforcement**
 - **BIS:** \$300 million penalty against Seagate Technology
 - **OFAC:** Substantial multi-million-dollar settlements against fintech, crypto, and blockchain companies.
 - **CBP:** Withhold/Release Order against Shanghai Select Safety Products (work gloves)



UK and EU Trade Risks and Enforcement Trends

UK - OFSI

- Taken enforcement action against 9 companies since 2019 (penalties ranging from £5,000 to £20 million)
- Enforcement team has recently grown by 175%
- 172 cases under investigation
- First enforcement action regarding post-2022 Russian sanctions 'expected in 2024'
- As of October 2023, £22.7 billion worth of assets were frozen under the post-2022 Russian sanctions

EU

- Recently introduced EU-wide standards for criminalizing sanctions violations
- EU Sanctions Whistleblower Tool – voluntary and anonymous reporting of EU sanctions violations to the EU commission

What can US, foreign, and multinational companies do?

- Build, review, and regularly update tailored, risk-based compliance programs
 - Identify business units or regions that warrant heightened diligence
 - Keep good records
- Regularly train employees, including those not in legal or compliance functions
 - Sales, procurement, and finance employees can be early warning systems
- Conduct diligence on counterparties and require suppliers to conduct diligence up the supply chain
 - Do not stick your “head in the sand” regarding sub-contractors, sub-distributors, etc.
- Understand where and how your supply chain has exposure to risky countries or counterparties
- Maintain open lines of communication with your banks to facilitate their reviews of your transactions
- Stay abreast of trade developments in any country where you operate, source supplies, or make sales
- Understand reporting obligations for breaches of sanctions and export controls



Questions or Comments?



Shoba Pillay

Partner | Chicago
spillay@jenner.com
+1 312 923 2605



Rob Dalling

Partner | London
rdalling@jenner.com
+44 330 060 5447



Alexis Early

Partner | Washington, DC
aearly@jenner.com
+1 202 639 6866

CLE RELAY

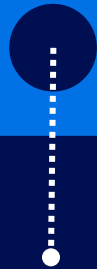
FULL SCHEDULE

JENNER & BLOCK



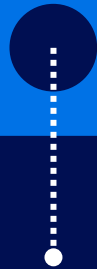
Session 1
Inputs and Outputs: The State of Play in Year Two of Generative AI

Friday, May 10
12 pm CT



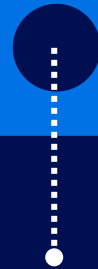
Session 2
One Year Later: DEI in a Post-SFFA World

Friday, May 17
12 pm CT



Session 3
Hot Topics in Fintech and Crypto

Friday, June 7
12 pm CT



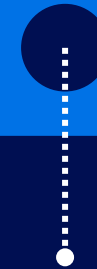
Session 4
How to Navigate Government Scrutiny from Regulators and Legislatures Worldwide

Friday, June 14
12 pm CT



Session 5
Global Enforcement Trends and Emerging Risks in Sanctions, Export Control, and Supply Chain

Friday, June 21
12 pm CT



Session 6
Information Exchanges: Navigating Antitrust Risk Without Safe Harbors

Tuesday, June 25
12 pm CT



Session 7
US Supreme Court Term in Review

Friday, June 27
12 pm CT