

CLIENT ALERT

# U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

January 17, 2023

## AUTHORS

David Mortlock | Britt Mosman | Michael J. Gottlieb | William J. Stellmach  
Joshua Nelson

Last year was a watershed moment for sanctions and export controls, as the Biden administration and its allies hammered Russia with round after round of novel and sweeping sanctions and export controls in response to Russia's invasion of Ukraine. Sanctions continued to be the U.S. government's tool of choice in response to a range of foreign policy challenges, including concerns about China and a "whole-of-government" review of cryptocurrency. However, the spotlight also turned to export controls in 2022, as one of the most powerful tools that the United States has leveraged in response to Russia's invasion of Ukraine and China's technological rise.

This alert covers the following topics:

➤ **Russia Sanctions**

In 2022, sanctions featured prominently in the U.S. and international response to Russia's invasion of Ukraine. The United States worked closely with the United Kingdom ("**UK**"), the European Union ("**EU**"), and other allies to deploy sanctions that curbed the ability of the Russian government to fund its war effort and export controls that prevented the Russian armed forces from accessing essential items for combat and maintenance.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

### ➤ **Governmental Focus on Cryptocurrency**

Cryptocurrency's entrance into the mainstream resulted in a greater risk of misuse for sanctions evasion and money laundering. The Biden administration responded by initiating a whole-of-government review focusing on digital assets. While digital assets have been subject to a patchwork of regulatory regimes and enforcement to date, a unified approach to these products is a necessary hurdle, as they continue to make headway into finance and the public consciousness.

### ➤ **The use of the Foreign Direct Product Rule to Supplement Russian Sanctions and to Target China**

The U.S. Commerce Department's Bureau of Industry and Security ("**BIS**") has employed the foreign direct product rule to limit the Russian and Belarusian armed forces' access to military technology. In addition, as competition with China reached new heights, BIS used export controls to limit China's access to U.S.-origin critical technologies for semiconductor manufacturing and deployed the foreign direct product rule to prevent China from looking elsewhere to source necessary products.

### ➤ **Additional Developments**

While the Russian invasion of Ukraine dominated the sanctions landscape in 2022, the United States also continued to use sanctions as a foreign policy tool to address national security issues and human rights abuses abroad, imposing sanctions in Ethiopia and Nicaragua, as well as maintaining sanctions regimes elsewhere. The trend of increasing cross-government enforcement actions and investigations also continued this year.

#### **A. United States uses sanctions as the tool of choice against Russia and Belarus in response to the war in Ukraine and other harmful foreign activities**

The Biden administration imposed sweeping new sanctions on Russia in response to Russia's invasion of Ukraine. Prior to the invasion, the United States had imposed sanctions measures targeting the Russian economy in response to previous acts of Russian aggression. Executive Order ("**E.O.**") [14024](#), signed in 2021, authorizes the U.S. Department of Treasury's ("**Treasury**") Office of Foreign Assets Control ("**OFAC**") to designate persons involved in Russian malicious cyberattacks, election interference, corruption, and assassination, among other things. In February 2022, OFAC promulgated 31 CFR Part 587, the Russian Harmful Foreign Activities Sanctions Regulations, to implement E.O. 14024. OFAC has historically used this E.O. to target Russian actors involved in election interference, but in 2022, OFAC used it as the foundational authority for its response to Russia's invasion of Ukraine.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

As the war in Ukraine has progressed, the United States has imposed increasingly strict sanctions on Russia and Belarus. Sanctions targeted areas critical for Russia's ability to fund its war effort, such as financial institutions, sovereign debt, and oil and gas. Additionally, restrictions in areas like services, luxury imports

and exports, and personal sanctions against Putin and his close allies all make up important components of the economic response to Russia's invasion of Ukraine, further limiting Russia's access to the global economy. As the war continues, the United States has imposed additional sanctions as it identifies other economic areas supporting the war effort, such as the price cap on Russian oil that took effect on December 5, 2022.<sup>1</sup> In October 2022, a joint alert from the Departments of Treasury, Commerce, and State put it plainly: "The strategic intent of our actions is to degrade Russia's ability to wage its unjust war against Ukraine and prevent Russia from projecting military force beyond its borders."<sup>2</sup>

---

*The strategic intent of our actions is to degrade Russia's ability to wage its unjust war against Ukraine and prevent Russia from projecting military force beyond its borders.*

DEPARTMENTS OF TREASURY, COMMERCE, AND STATE JOINT ALERT

---

Notably, the United States imposed sanctions on Russia in coordination with the UK, the EU, and other allies. However, throughout the course of the war, the ongoing response of each jurisdiction has, and will likely continue to, diverge. Companies can no longer assume that compliance with U.S. sanctions ensures compliance with those imposed by the EU and the UK. For example, the UK has frozen the assets of several prominent Russian oligarchs, including Roman Abramovich, not yet designated by the United States.

Current U.S. sanctions targeting Russia for its invasion of Ukraine can broadly be divided into five areas: (1) comprehensive sanctions on Russian occupied territory in Ukraine; (2) financial institutions; (3) industrial entities and products; (4) individuals; and (5) services, foreign investment, and consumer products. In addition, the United States imposed sanctions targeting Belarus for facilitating Russia's war.

### 1. Comprehensive Sanctions

In a significant escalation of the crisis, Russia's President Vladimir Putin announced his recognition of the Donetsk and Luhansk People's Republics ("**DNR**" and "**LNR**," respectively) as "independent" states in February 2022.

As an initial response, President Biden signed [E.O. 14065](#) imposing comprehensive sanctions on the DNR and LNR regions (the "**Covered Regions**") and potentially other regions in Ukraine. E.O. 14065 prohibits: (i) new investment in the

---

<sup>1</sup> Department of the Treasury, Determination Pursuant to Section 1(a)(ii) of Executive Order 14071, Prohibitions on Certain Services as They Relate to the Maritime Transport of Crude Oil of Russian Federation Origin, Nov. 21, 22, available [here](#); OFAC Guidance on Implementation of the Price Cap Policy for Crude Oil of Russian Federation Origin, November 22, 2022, available [here](#).

<sup>2</sup> Treasury-Commerce-State Alert: Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex, October 14, 2022, available [here](#).

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

Covered Regions, by a U.S. person, wherever located; (ii) the importation into the United States, directly or indirectly, of any goods, services, or technology from the Covered Regions; (iii) the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods, services, or technology to the Covered Regions; and (iv) any approval, financing, facilitation, or guarantee by a U.S. person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited if performed by a U.S. person.

### 2. Financial Institutions

U.S. sanctions on Russian financial institutions have steadily increased following Russia's invasion of Ukraine to target major banks, sovereign debt, government of Russia financial entities, and Russia's sovereign wealth fund. Each of these categories of sanctions attempts to target Russian efforts to fund its invasion.

**Sberbank.** The sanctions on Sberbank have evolved over the course of the conflict in Ukraine. While the first tranche of sanctions against Sberbank imposed prohibitions only on U.S. financial institutions and certain debt and equity transactions involving Sberbank, OFAC has since imposed full blocking sanctions on Sberbank. On April 6, 2022, OFAC designated Sberbank, placing it, along with 42 subsidiaries, on the SDN List. This action supersedes the prior sanctions prohibitions imposed on Sberbank and its subsidiaries. As a result of sanctions, several European subsidiaries of Sberbank, including entities indirectly owned by Sberbank, have been sold to other entities that are not the target of sanctions in order to avoid U.S., EU, and UK sanctions.

**Other major banks.** On February 24, 2022, OFAC designated several major Russian financial institutions pursuant to E.O. 14024, including VTB, VEB, Promsvyazbank PJSC, PJSC Bank Financial Corporation Otkritie, OJSC Sovcombank, JSC Bank Novikom, and a number of subsidiaries, including subsidiaries outside of Russia and some that operate in various other sectors. On April 6, 2022, OFAC designated Alfa-Bank and six of its subsidiaries and five vessels owned by one of Alfa-Bank's subsidiaries. On May 8, 2022, OFAC designated JSC Moscow Industrial Bank, along with 10 subsidiaries pursuant to E.O. 14024.

On February 24, 2022, OFAC also issued Directive 3 to E.O. 14024, which expands restrictions on new debt and equity transactions related to certain identified Russian entities. Specifically, Directive 3 prohibits U.S. persons from all transactions in, provision of financing for, and dealings in new debt of longer than 14 days' maturity and new equity of listed Russian entities, including Credit Bank of Moscow Public JSC and Gazprombank JSC.

**Prohibition on dealing in sovereign debt.** On February 22, 2022, the Biden administration, pursuant to Directive 1A under E.O. 14024, expanded existing restrictions in place on dealing in Russian sovereign debt on the primary market to also restrict participation in the secondary market.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

**Restrictions on credit to government of Russia financial entities.** On February 28, 2022, OFAC issued Directive 4 to E.O. 14024, the so-called “Sovereign Transactions Directive,” which prohibits U.S. persons from any transaction involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation, including any transfer of assets to such entities or any foreign exchange transaction for or on behalf of such entities, absent a license or authorization from OFAC. In contrast to most other OFAC sanctions and directives, the 50% rule does not apply to Directive 4. This means that U.S. persons are not prohibited from entering into transactions with entities owned by one of the three government entities listed above so long as no other sanctions or Directives are implicated.

**Blocking the sovereign wealth fund.** On February 28, 2022, OFAC announced new designations targeting Russia’s sovereign wealth fund, the Russian Direct Investment Fund. OFAC also designated its managing company, JSC Management Company of the Russian Direct Investment Fund; the managing company’s subsidiary, LLC RVC Management Company; and its Chief Executive Officer Kirill Dmitriev.

### 3. Industrial Entities and Products

U.S. sanctions in Russian industrial sectors have attempted to accomplish two goals: first, to restrict funding for the Russian invasion by limiting the sale of Russian export products like oil, gas, coal, and diamonds; and second, by restricting Russian defense and media companies’ access to the U.S. financial system.

**Nord Stream 2.** In line with German Chancellor Scholz’s move to suspend certification of Nord Stream 2, the Biden administration added Nord Stream 2 AG and its CEO, Matthias Warnig, to the SDN List on February 23, 2022.

**Import ban on Russian oil and gas.** On March 8, 2022, President Biden signed [E.O. 14066](#) prohibiting the importation into the United States of crude oil, petroleum, petroleum fuels, oils and products of their distillation, liquefied natural gas, coal, and coal products of Russian origin, as well as new investment in the energy sector in the Russian Federation by a U.S. person, wherever located.

**Other industrial entities.** On March 24, 2022, OFAC designated several major Russian defense companies, including Tactical Missiles Corporation JSC, JSC NPO High Precision Systems, NPK Tekhmash OAO, Joint Stock Company Russian Helicopters, and Joint Stock Company Kronshtadt, as well as many of their subsidiaries. OFAC also designated LLC Promtekhlogiya, a private defense company, on May 8, 2022. On April 7, 2022, OFAC designated several state-owned enterprises, including diamond-mining company Alrosa. On May 11, 2022, OFAC designated state-owned television stations JSC Channel One Russia, Television Station Russia-1, and JSC NTV Broadcasting Company.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

### 4. Individuals

The Biden administration announced sanctions on President Putin on February 25, 2022, and individuals, along with their family members, identified as having close personal ties with President Putin. These individuals include senior government officials, such as Minister of Foreign Affairs, Sergei Lavrov, and senior executives at significant state-owned and influential enterprises. On March 3, 2022, OFAC issued another significant series of designations targeting Russian billionaire affiliates of President Putin.

Notably, OFAC designated Alisher Usmanov, who owns significant interests in the metals and mining and technology sectors in Russia. Alongside the designation of Usmanov, however, OFAC issued General License 15, which authorizes transactions with any entity in which Usmanov owns a 50% or greater interest that is not itself listed on the SDN List.

On March 24, 2022, OFAC designated 328 members of the Russian State Duma and Herman Gref, the head of Sberbank, in line with actions taken by the UK, the EU, and Canada. On April 6, 2022, OFAC designated President Putin's adult daughters and Lavrov's wife and adult daughter, along with several members of Russia's Security Council. On May 8, 2022, OFAC designated the First Deputy Chairman of the Executive Board of Sberbank and the Board of Directors of Gazprombank.

### 5. Services, Foreign Investment, and Consumer Products

On April 6, 2022, President Biden signed [E.O. 14071](#), prohibiting new investment in the Russian Federation by a U.S. person, wherever located. In a novel use of sanctions, E.O. 14071 also prohibits the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a U.S. person, of any category of services as may be determined by the Secretary of the Treasury to any person located in the Russian Federation. The Secretary of the Treasury determined that the provision by U.S. persons of accounting, trust and corporate formation, and management consulting services are prohibited under the E.O. In addition, the authorization lays the groundwork for Treasury to potentially restrict additional categories of services, multiple categories of services, or the provision of services to the entire Russian economy in the future.

On March 11, 2022, President Biden signed [E.O. 14068](#), prohibiting the following activities: (1) the importation into the United States of Russian-origin fish, seafood and preparations thereof, alcoholic beverages, and non-industrial diamonds; (2) the exportation of luxury goods to Russia, as to be described by the U.S. Department of Commerce and currently including certain spirits, tobacco products, clothing items, jewelry, vehicles, and antique goods; and (3) the exportation of U.S. dollar-denominated banknotes to Russia.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

### 6. Sanctions Targeting Belarus

In response to Belarus's facilitation of Russia's invasion of Ukraine, President Biden announced a new tranche of sanctions targeting the Lukashenka regime in Belarus, with the designation of 24 Belarusian persons, including state-owned banks major companies in and the defense and security industries. The international community subjected the Lukashenka regime to multiple rounds of sanctions targeting corruption during elections and as a response to the 2021 diversion of a civil aircraft in order to arrest a Belarussian dissident.

#### **B. Sanctions concerns are key in President Biden's whole of government review of cryptocurrency and enforcement actions**

The rise in prominence of cryptocurrencies and other digital assets has created an attractive avenue for bad actors to circumvent sanctions and launder money. This (among other concerns) prompted the Biden administration to initiate a whole-of-government review of its approach to digital assets in order to increase consistency between agencies and resolve potential loopholes in areas like sanctions and money laundering. While this was an issue before the Russian invasion of Ukraine, as highlighted by the laundering of \$8 billion through cryptocurrency exchange Binance to Iran,<sup>3</sup> OFAC continued targeting bad actors in the cryptocurrency space, including entities involved in the Russian cryptocurrency mining industry.<sup>4</sup>

#### **1. Biden administration calls for whole-of-government review of approach to digital assets and cryptocurrencies**<sup>5</sup>

On March 9, 2022, President Biden issued [E.O. 14067](#) entitled "Ensuring Responsible Development of Digital Assets" in response to the explosive growth of the digital asset and cryptocurrency sectors, which have grown from a cumulative \$14 billion market capitalization to \$3 trillion in just the last five years.<sup>6</sup> E.O. 14067 outlines the nation's first whole-of-government approach to evaluating the risks and potential benefits of digital assets. This approach follows individual agencies' attempts to regulate digital assets, such as OFAC's October 2021 Sanctions Compliance Guidance for the Virtual Currency Industry.<sup>7</sup> Like many executive orders, E.O. 14067 serves a messaging function to indicate the Biden

---

<sup>3</sup> Angus Berwick and Tom Wilson, Crypto Exchange Binance Helped Iranian Firms Trade \$8 Billion Despite Sanctions, Reuters, November 7, 22, available [here](#).

<sup>4</sup> See Congressional Research Service, Russian Sanctions and Cryptocurrency, May 4, 2022, available [here](#); U.S. Treasury Designates Facilitators of Russian Sanctions Evasion, Office of Foreign Assets Control, April 20, 2022, available [here](#).

<sup>5</sup> For more information on this topic, please see our prior client alerts, "Biden Administration Calls for Whole-of-Government Review of Approach to Digital Assets," available [here](#), and "New Reports Outline Recommendations to Advance Comprehensive Framework for Regulation of Digital Assets," available [here](#).

<sup>6</sup> Press Release, The White House Executive Order on Ensuring Responsible Development of Digital Assets March 9, 2022, available [here](#); and White House Fact Sheet, March 9, 2022, available [here](#).

<sup>7</sup> Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry, October 2021, available [here](#).



---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

administration's broad view of digital assets. As a messaging document, the Order is an important step in Washington's policy response to the emergence of a revolutionary new architecture of digital money and distributed finance.

Among other things, the Biden administration cautioned that the United States must mitigate the illicit finance and national security risks resulting from the misuse of digital assets such as through money laundering, cybercrime, human trafficking, and other methods. E.O. 14067 also highlighted the potential for sanctioned persons to rely upon digital assets to circumvent U.S. and foreign sanctions regimes. The Order notes that when cryptocurrencies are misused, there is a significant threat to the national security of the United States, and calls on numerous agencies to provide a report devising a plan for mitigating crypto-specific illicit finance and national security risks while preserving the efficacy of the United States' national security tools.

The Order calls for action from nearly all of the federal financial regulators, various departments of the U.S. Cabinet (including Treasury, State, Justice, and others), the Office of Science and Technology Policy, the Director of National Intelligence, and a number of other agencies and officials to help mitigate the illicit finance and national security risks resulting from the misuse of cryptocurrencies. These risks include (among others) the risk that cryptocurrencies may be the means by which sanctions targets circumvent U.S. and foreign sanctions regimes. For example, E.O. 14067 notes that illicit actors often launder and cash out their illicit proceeds using cryptocurrency service providers, such as cryptocurrency exchanges, in jurisdictions that have not yet effectively implemented the international standards set by the Financial Action Task Force. Therefore, the continued availability of service providers in such jurisdictions supports financial activity without illicit finance controls.

### 2. Cryptocurrency factors into sanctions policy<sup>8</sup>

As detailed above, the United States and its allies have responded to Russia's invasion of Ukraine by imposing sanctions that isolate large numbers of Russian actors from the global financial and trade system. Certain features of cryptocurrencies and their underlying technologies may initially appear to make the asset class attractive to persons that are blocked from the traditional U.S. financial system. However, the U.S. government has shown that it has the capability to track and find stolen cryptocurrency, such as the proceeds of the 2016 hack of Bitfinex<sup>9</sup> and the Colonial Pipeline ransom,<sup>10</sup> and can apply this expertise to identifying and enforcing cryptocurrency-related sanctions violations. In the past

---

<sup>8</sup> For more on this topic, please see our prior client alert, "Will Crypto Make a Hash of the Sanctions Against Russia?" available [here](#).

<sup>9</sup> Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency, U.S. Department of Justice Press Release, February 8, 2022, available [here](#).

<sup>10</sup> Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, U.S. Department of Justice Press Release, June 7, 2021, available [here](#).



---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

few years, OFAC has increasingly imposed blocking sanctions on persons that have used virtual currency in connection with malign activity.<sup>11</sup>

Some members of the U.S. government have expressed concern that cryptocurrencies may offer sanctions targets and other illicit actors an alternative means of facilitating transactions due to their ease of transferability, transaction anonymity, and decentralization features.<sup>12</sup> In 2022, these concerns became even more urgent after reports that Russian entities were preparing to use cryptocurrencies to blunt the effect of sanctions imposed after the invasion of Ukraine.<sup>13</sup> Indeed, Russia's largest financial institution, Sberbank, reportedly received a license from the Russian Central Bank to issue digital assets to clients in March 2022, a significant departure from Russia's pre-war crypto stance.<sup>14</sup> A 2021 report prepared by Treasury noted how technological innovations, such as cryptocurrencies, potentially reduce the efficacy of American sanctions since crypto transactions offer malign actors opportunities to hold and transfer funds outside the traditional dollar-based financial system.<sup>15</sup> In addition, on March 2, 2022, Senators Warren, Warner, Brown, and Reed wrote to U.S. Treasury Secretary Janet Yellen voicing concerns about Treasury's progress in monitoring and enforcing sanctions compliance within the cryptocurrency industry, especially given the need to ensure the efficacy and integrity of U.S. sanctions against Russia.<sup>16</sup>

However, these concerns may not be as widespread as initial reports suggested. On March 8, 2022, a senior Biden administration official said, "[on] Russia, in particular, the use of cryptocurrency we do not think is a viable workaround to the set of financial sanctions we've imposed across the entire Russian economy and, in particular, to its central bank."<sup>17</sup>

---

<sup>11</sup> Historically, this has been used for hacking-related activities. For example, in September 2021, OFAC designated SUEX OTC, S.R.O. ("**SUEX**"), a Russian virtual currency exchange, for facilitating financial transactions for ransomware actors. An analysis of SUEX transactions highlighted that over 40% of SUEX's known transaction history was associated with illicit actors. In addition, OFAC has designated various Russian entities associated with certain malware and malware-related cyberattacks, such as Evil Corp—the Russia-based cybercriminal organization behind the Dridex malware.

<sup>12</sup> Russian Sanctions and Cryptocurrency, Congressional Research Service, May 4, 2022, available [here](#); Treasury 2021 Sanctions Review, *infra* at note 8; Letter to Treasury re OFAC crypto sanctions enforcement, *infra* at note 9.

<sup>13</sup> Emily Flitter and David Yaffe-Bellany, Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions, The New York Times, Feb. 23, 2022, available [here](#).

<sup>14</sup> Will Daniel, Russian banks are so broke the biggest lender just got the go-ahead to issue digital assets like crypto, Fortune, Mar. 18, 2022, available [here](#).

<sup>15</sup> Department of the Treasury, The Treasury 2021 Sanctions Review, Oct. 2021, available [here](#).

<sup>16</sup> United States Senate, Letter to Treasury re OFAC crypto sanctions enforcement, Mar. 2, 2022, available [here](#).

<sup>17</sup> Press Briefing, Background Press Call by Senior Administration Officials on the President's New Digital Assets Executive Order, Mar. 8, 2022, available [here](#).

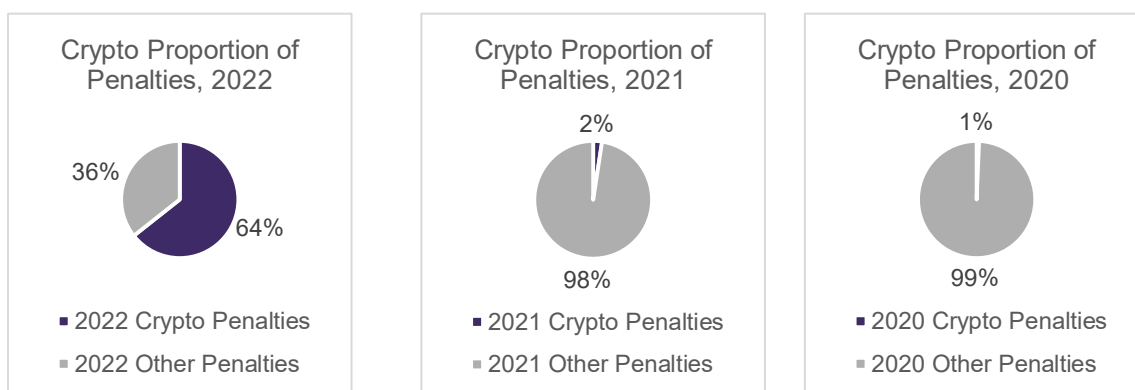
---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

This sentiment was echoed by Carole House, Director of Cybersecurity and Secure Digital Innovation for the National Security Council and Him Das, Acting Director of Treasury's Financial Crimes Enforcement Network ("FinCEN").<sup>18</sup>

### 3. Highlighting Crypto-Enforcement Actions and Designations in 2022

In addition to the Biden administration's focus on closing national security gaps caused by the rapid rise of cryptocurrency, OFAC has continued its crackdown on sanctions violations related to the cryptocurrency sphere. From its first crypto-related enforcement action in 2020 against BitGo,<sup>19</sup> where OFAC assessed \$98,830 in civil penalties, to 2021's BitPay action (\$507,375),<sup>20</sup> to 2022's Bittrex action (\$24,280,829.20)<sup>21</sup> and Payward, Inc. action (\$362,158.70),<sup>22</sup> civil penalties have increased exponentially. OFAC has also increased enforcement in the digital currency space. This year, OFAC designated two Russia-based entities that use digital currencies to facilitate criminal activity, Hydra, the world's largest darknet market, and Garantex, a virtual currency exchange used to facilitate Russian ransomware and darknet projects. Two of the year's most important crypto enforcement actions were the designation of Tornado Cash, a virtual currency mixer, and a joint enforcement action with FinCEN against Bittrex, a virtual currency exchange. Crypto's increasing role in OFAC enforcement is reflected by the increased share of penalties coming from crypto-related actions:



---

<sup>18</sup> Hannah Lang, U.S. lawmakers push Treasury to ensure Russia cannot use cryptocurrency to avoid sanctions, Reuters, Mar. 2, 2022, available [here](#). Him Das: "Although we have not seen widespread evasion of our sanctions using methods such as cryptocurrency, prompt reporting of suspicious activity contributes to our national security and our efforts to support Ukraine and its people." Immediate Release, FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts, Mar. 7, 2022, available [here](#).

<sup>19</sup> OFAC Enters Into \$98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transaction, Dec. 30, 2020, available [here](#).

<sup>20</sup> OFAC Enters Into \$507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transaction, Feb. 18, 2021, available [here](#).

<sup>21</sup> OFAC Enters Into \$24,280,829.20 Settlement with Bittrex, Inc. for Apparent Violations of Multiple Sanctions Programs, Oct. 11, 2022, available [here](#).

<sup>22</sup> OFAC Settles with Virtual Currency Exchange Kraken for \$362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations, Nov. 28, 2022, available [here](#).

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

### a. **OFAC designates Tornado Cash for laundering the proceeds of cybercrimes, including for North Korean state-sponsored hacking group**<sup>23</sup>

On August 8, 2022, OFAC designated Tornado Cash, a virtual currency mixer, for laundering the proceeds of cybercrimes, including crimes committed against U.S. victims. OFAC reports that Tornado Cash indiscriminately facilitates anonymous virtual currency transactions while making no attempt to determine their origin and is accused of laundering more than \$7 billion worth of virtual currency since its creation in 2019. This includes the laundering of \$455 million stolen by the Lazarus Group as part of the largest-known virtual currency heist to date. The Lazarus Group, a state-sponsored hacking group in the Democratic People's Republic of Korea (DPRK), was sanctioned by the United States in 2019. According to OFAC, Tornado Cash is also allegedly responsible for laundering more than \$96 million from the June 24, 2022 Harmony Bridge Heist and approximately \$7.8 million from the August 2, 2022 Nomad Heist.

Similar to OFAC's designation of virtual currency mixer Blender.io on May 6, 2022, OFAC sanctioned Tornado Cash pursuant to E.O. 13694, as amended, for providing material, financial, or technological support to a cyber-enabled activity that originated outside of the United States and contributed to a significant threat to the national security, foreign policy, or economic health of financial stability of the United States.

On September 8, 2022, six plaintiffs filed a complaint in the U.S. District Court for the Western District of Texas challenging the decision by OFAC to add Tornado Cash to the SDN List. The plaintiffs—all individuals who have used Tornado Cash for legitimate purposes and whose crypto assets remain locked in Tornado Cash smart contracts since the August 2022 designation—accuse Treasury of engaging in an “unprecedented, overbroad action” which exceeds its statutory authority, infringes upon their constitutional rights, and “threatens the ability of law-abiding Americans to engage freely and privately in financial transactions.”<sup>24</sup>

### b. **Bittrex fails to implement effective anti-money laundering program, facilitates \$263 million worth of crypto transactions to embargoed countries**

On October 11, 2022, OFAC announced that it reached a settlement with Bittrex, Inc., a Seattle-based private company that provides an online virtual currency exchange and hosted wallet services. Under the settlement, Bittrex agreed to pay more than \$24 million to resolve its potential civil liability for 116,421 apparent violations of Ukraine-related sanctions and sanctions against Cuba, Iran, Sudan, and Syria. This settlement is part of a global resolution with FinCEN which, under a separate settlement, assessed a civil money penalty of more than \$29 million against Bittrex for the company's failure to implement an effective anti-money laundering program between February 2014 and December 2018, in violation of the Bank Secrecy Act and FinCEN's implementing regulations. Under the terms of the FinCEN settlement, FinCEN will credit

---

<sup>23</sup> For more information on this topic, please see our Compliance Concourse podcast, “OFAC Sanctions on Tornado Cash: We're Not in Kansas Anymore,” available [here](#).

<sup>24</sup> Compl. 1-2, *Van Loon v. Treasury* (W.D. Tex. 2022) (6:22-cv-00920).

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

Bittrex for the \$24 million that it agreed to pay for the OFAC violations, requiring Bittrex to pay an additional \$5 million to resolve the anti-money laundering violations.

According to OFAC, between March 2014 and December 2017, Bittrex failed to prevent approximately \$263 million worth of virtual currency-related transactions on its platform by users located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria because the company had an inadequate sanctions compliance program. While Bittrex started offering virtual currency services in March 2014, the company allegedly had no sanctions program in place until December 2015, when it began verifying customers' identities. Months later, in February 2016, Bittrex retained a third-party vendor to perform sanctions screening. However, in October 2017, when OFAC launched its investigation into potential sanctions violations, Bittrex discovered that the vendor's screening was incomplete, and the vendor had only been checking transactions against persons who appeared on OFAC's SDN List and failed to determine if Bittrex customers or transactions were connected to sanctioned jurisdictions. Bittrex also failed to screen customer Internet protocol addresses and physical addresses until October 2017, even though Bittrex had collected this information from customers at onboarding.

OFAC indicated that the \$24 million settlement amount was based upon its determination that the apparent violations were not voluntarily self-disclosed by Bittrex and were not egregious in nature. Following its investigation, OFAC also determined that Bittrex implemented a number of remedial measures, including hiring additional compliance staff, conducting additional sanctions compliance training, and implementing new sanctions screening and blockchain tracing software, which, according to OFAC, had substantially curtailed the number of apparent violations.

### **C. Foreign direct products rule reforms expand the reach of U.S. export controls**

Export controls have risen in prominence as a powerful economic tool for the United States to exert influence abroad. One of the most influential tools for expanding the reach of export controls has been the Foreign Direct Product Rule ("FDPR"). The FDPR allows the United States to assert jurisdiction over products produced outside its borders when those products are the result of technology or software that is subject to the Export Administration Regulations ("EAR"). The United States has used the FDPR in recent moves to pressure Russia and Belarus and to attempt to control the technological rise of China. The broad scope of the FDPR allows the United States to limit access to prohibited end-users and end uses for products that bear a limited connection to the United States. While other governments, such as the UK and the EU, have also enacted harsh economic measures against Russia, future use of the FDPR in areas of less international consensus may expose non-U.S. exporters to inconsistent and conflicting rules in the future.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

The prominence of export controls has dovetailed with the use of sanctions as an economic tool to exert international influence. The Russia/Belarus FDPs, discussed below, were imposed in concert with sanctions to hamper the war effort and impact the domestic economy.<sup>25</sup>

### 1. Russian and Belarussian FDP measures

The items subject to the new Russia/Belarus export control rule include sophisticated technologies designed and produced in the United States, in addition to certain foreign-produced items that contain or are based on U.S.-origin technology subject to the EAR or other technology that is subject to the EAR that are essential inputs to Russia's and Belarus's key technology and other sectors, in particular, the defense, aerospace, and maritime sectors.

The Russia/Belarus FDP established a license requirement for foreign-produced items that meet certain product scope and destination scope requirements described in Section 734.9(f) of the EAR. The Russian/Belarus FDP made several articles controlled for export under the EAR the "direct product" of a wide range of Commerce Control List ("CCL") software and technology, or items produced by a complete plant or a major component of a plant that itself is the direct product of such U.S.-origin technology or software, when it is known that the foreign-produced item is destined for Russia or Belarus or will be incorporated into or used in the production or development of any part, component, or equipment produced in or destined for Russia or Belarus. Notably, the product scope of the Russia/Belarus FDP does not include items designated EAR99 that are produced by software or technology as described in Section 734.9(f)(1)(i) or by a complete plant or major component of a plant as described in Section 734.9(f)(1)(ii).

Under the new rule, "any destination" is used to address situations involving multi-step manufacturing processes that occur in more than one country and in which the parties involved have knowledge that the foreign-produced item being produced will ultimately be destined for Russia or Belarus. For example, this means that the licensing requirements will apply to exports and reexports from abroad from manufacturing country 1 to manufacturing country 2 (each contributing to the production chain) when there is knowledge that the reexport or export from abroad of the item is ultimately destined for Russia or Belarus or will be incorporated into or used in the production of any part, component, or equipment (not designated EAR99) produced in or ultimately destined for Russia or Belarus.

As part of the new Russia/Belarus military end-user ("MEU") FDP rule, the Bureau of Industry and Security ("BIS") expanded the scope of the existing "military end-use" and "military end-user" control under Section 744.21 of the EAR for Russia and Belarus supply chain items subject to the EAR except for food and medicine designated EAR99.

Companies outside the United States should be mindful of the FDP. Pursuant to the FDP, certain U.S. export controls also apply to foreign products manufactured using certain U.S. technology or software. As a result, non-U.S. companies

---

<sup>25</sup> Treasury-Commerce-State Alert: Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex, October 14, 2022, available [here](#).

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

may be affected if they rely on U.S. technology when manufacturing goods. The FDPR is currently suspended with respect to exports from countries that have imposed export controls against Russia that are similar to the U.S. export controls. The FDPR thus currently does not apply to many U.S. allies, including the EU member states and the UK.<sup>26</sup> However, non-U.S. companies must observe the FDPR if, for example, products are exported to Russia via a subsidiary in a country that is not exempt from the FDPR.

### **2. Countering China's advancement in technology and maintaining U.S. supremacy**

The approach to export controls for China has been a mix of traditional export control restrictions targeting the Chinese military and other potentially malign actors, such as adding Chinese businesses to the Entity List, and the expansion of the FDPR to limit China's access to semiconductor and supercomputer development. The United States complemented its mixed approach with sanctions, including regulations promulgated in February 2021 to limit securities investment in Chinese military companies by creating the Non-SDN Chinese Military-Industrial Complex Companies ("**NS-CMIC**") list.<sup>27</sup>

#### **a. United States limits Chinese semiconductor growth through export control restrictions**

As part of a far-reaching package of new rules intended to increase pressure on China and maintain American technological leadership, the U.S. Department of Commerce ("**Commerce**") once again expanded the reach of the FDPR for exports to China while also adding new classes of controlled products and restrictions on U.S. person support for the development or production of certain integrated circuits. The new rules, released on October 7, 2022, are designed to halt exports to China of a variety of advanced computing and semiconductor-related items and to prevent China from acquiring the means to produce high-end computer chips on its own. The United States believes semiconductors and supercomputers are of vital national security importance and seeks to prevent China from surpassing U.S. industry in these areas.

Specifically, the new rules add certain advanced computing chips, semiconductor manufacturing equipment, and associated technology to new CCL categories; establish new end-use controls for certain items on the CCL; and expand the scope of the FDPR, addressing entities on the Entity List to cover those items and to include additional end-users.

The new regulations then impose further controls on a variety of exports based on their end-use. Specifically, Commerce establishes a presumption of denial for license requests for end-users in China for "semiconductor manufacturing equipment" and so-called "supercomputers" when certain conditions are met. For manufacturing equipment-related exports, the new rules impose a license requirement under a presumption of denial.

---

<sup>26</sup> 15 C.F.R. 746 Supp. 3. Also currently exempt are Australia, Canada, Japan, South Korea, New Zealand, Norway, and Switzerland.

<sup>27</sup> See Executive Order 14032, Jan. 13, 2021, available [here](#).

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

These new regulations represent a significant expansion of U.S. export controls on China. In addition, they may signify the path Commerce intends to take with respect to China going forward, presaging ever greater controls over industries where the United States views Chinese competition as a strategic and national security threat (such as biotechnology). For now, the new rules expand Commerce's controls over new categories of semiconductors, computers, and related products and expand the scope of the behaviors and products over which Commerce claims jurisdiction. Companies involved in high technology will need to parse both the rules and their operations to ensure continued compliance and navigate Commerce's ever more complex licensing regime.

### a. Chinese FDPR measures

The new Chinese export control rules discussed above build on the FDPR that Commerce has increasingly used as an export control tool. The FDPR prohibited the export, first to Huawei and its subsidiaries, and then to entities in Russia and Belarus, of certain foreign-produced items that were the direct product of, or the direct product of a plant or major component of a plant that was itself the direct product of, certain specified U.S.-origin technology or software. As the United States continues to take a broader view of what encompasses a national security risk, the role of export controls will continue to grow. The FDPR is an especially prominent tool available to exert influence extraterritorially.

Unlike with Russia and Belarus, the FDPR for China does not restrict the export of all controlled items, but rather only for select technologies the United States deems critical to Chinese advancement or for certain end-users. With its most recent Chinese export control rulemaking, Commerce first expanded the FDPR to encompass both supercomputers (as defined above) and other "advanced computing" inputs. Accordingly, any of these items, even if they are foreign produced, that are either direct products of U.S. technology, or the direct product of a plant or major component of a plant that is a direct product of U.S. technology, now require a license for export to China. Second, Commerce expanded the scope of the so-called "Entity List FDPR" (EAR § 734.9(e)) which had previously applied primarily to Huawei and its subsidiaries. Commerce has now added an additional 28 Chinese entities (all already listed on the Entity List) to the revised end-user scope of the Entity List FDPR.

As with prior iterations of the FDPR, this newest expansion has had a broad impact on manufacturers across the supply chain. In addition to "know your customer" procedures, exporters who intend to send any of the newly controlled technology (or its equivalent) to the PRC would do well to also institute "know your provider" procedures in order to avoid running afoul of the expanded controls. The model compliance certificate will likely be one helpful tool, but manufacturers may need to conduct additional diligence across their commercial relationships. The U.S. person-related provisions described above dramatically raise the stakes for U.S. citizens or legal permanent residents involved at any stage of the semiconductor supply chain. Even if working abroad for a non-U.S. company, such persons need to confirm that their activities are not covered by the new license requirements.



---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

Moreover, even lack of knowledge of the end-use is not necessarily a defense for U.S. persons engaged in activity covered by the new rule. Under the U.S. person restrictions, even where the U.S. person is unsure of whether the integrated circuits being produced in China meet the technical specifications, a license is required. And, this negative presumption is mirrored in the new end-use restrictions as well, where even when an exporter does not know whether a semiconductor fabrication facility produces integrated circuits that meet the identified technical specifications a license is required.

### **D. Other Developments in Sanctions**

Beyond Russia, China, and cryptocurrency, OFAC has refined other areas of sanctions regulation. Among other things, OFAC issued sanctions to address the humanitarian and human rights crisis in Ethiopia; increased the scope of sanctions against Nicaragua's Ortega-Murillo regime; and reissued sanctions regulations for Libya, the Central African Republic, the Western Balkans, and Cyber Related Sanctions. OFAC has also increased its cooperation with other government entities to bring joint enforcement actions and continued its efforts towards coordinating its sanctions policies with those of allied nations.

On February 8, 2022, OFAC issued the Ethiopia Sanctions Regulations pursuant to its authority under [E.O. 14046](#), a response to the conflict in Ethiopia's northern Tigray region. The Ethiopia Sanctions Regulations implement E.O. 14046's restriction on persons responsible for or complicit in the Tigray conflict. Since the implementation of sanctions, the conflict has been halted under two ceasefires: the first ceasefire held from March to August 2022, the second is currently ongoing. Under the Ethiopia Sanctions Regulations, OFAC has sanctioned the Eritrean Defense Forces, the ruling party of Eritrea, two state-owned businesses, and associated individuals.

On October 24, 2022, President Biden signed [E.O. 14088](#), which took additional steps to address political repression and violence in Nicaragua. The United States has maintained a sanctions program against Nicaragua since its government violently responded to protests in April 2018. The initial sanctions program authorized OFAC to sanction human rights abusers and government officials of Nicaragua. President Biden's October 2022 expansion of the sanctions regime targeted the gold mining industry in Nicaragua, a major source of funding for the Ortega-Murillo government. Further, it authorized OFAC to sanction persons responsible for repressing freedoms of the press, assembly, and expression. OFAC issued regulations blocking the government entity responsible for administering the nation's gold mines and a close confidante of Nicaraguan President Ortega.

OFAC reissued and updated sanctions related to Libya, the Central African Republic, the Western Balkans, and its Cyber Related Sanctions Regulations. Each of these sanctions regulations included additional interpretive guidance and definitions and other general licenses and regulatory provisions to maintain these programs. However, OFAC did not make significant updates or changes to any of these programs.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

OFAC also continued to bring joint enforcement actions and investigations with other government entities, including FinCEN and the Department of Justice. As discussed above, OFAC and FinCEN cooperated on a \$29 million enforcement action against Bittrex for violations of the Bank Secrecy Act and the Ukraine, Cuba, Iran, Sudan, and Syria related sanctions issued by OFAC. Further, OFAC and the Department of Justice are coordinating an enforcement action regarding an apparent violation of the Iranian Transactions and Sanctions regulations by Turkish Halkbank, which is scheduled to be heard by the Supreme Court on January 17, 2023.<sup>28</sup>

Finally, OFAC has continued its push to coordinate its sanctions programs with key allies such as the UK. This furthers a trend that was established after Treasury's 2021 Sanctions Review, published in October of 2021, specifically noted that, where possible, sanctions "should be coordinated with allies, incorporating shared intelligence and resources, and accompanied by engagement with relevant stakeholders including industry, financial institutions, allies, civil society, and the media" in order to modernize OFAC's implementation of sanctions.<sup>29</sup> OFAC further demonstrated its emphasis on multilateral coordination during the October 17, 2022 joint statement announcing an enhanced partnership between OFAC and its UK counterpart, the Office of Financial Sanction Implementation ("**OFSI**").<sup>30</sup>

### **E. Conclusion**

Both within the U.S. government and with foreign regulatory bodies, cooperation has been a theme of the year. The rising importance of export controls in the economic toolbox has required increased coordination between OFAC and BIS. Furthermore, the U.S. government has worked closely with allies including the UK and the EU, to coordinate its sanctions and export control response. This cooperation has been a force multiplier—the united response to the Ukraine invasion, for instance, has allowed each government's program to have a greater impact on Russia than it would be otherwise because cooperation limits the ability of Russian actors to evade sanctions. Yet, this increased cooperation has also highlighted the divergence between governments and increased the demand on compliance teams. Whereas before, companies could generally meet their sanctions obligations to most applicable jurisdictions by complying with U.S. sanctions, now, companies must consider that other sanctions regimes may be more stringent than those implemented by the United States. While cooperation leads to greater effectiveness, it also increases the regulatory burden on international businesses. Moreover, the expansive view of national security embodied by sanctions and export control regulations will cause more businesses to review their obligations under those regulations.

We anticipate the trend of multilateral cooperation to continue into 2023, highlighted by the enhanced partnership between OFAC and OFSI. Additionally, we anticipate that, despite the trend of continued multilateral coordination, there may be more situations where either UK or EU restrictions are broader in scope than those imposed by the United States, as the

---

<sup>28</sup> See Supreme Court Docket No. 21-1450, *Turkiye Halk Bankasi A.S. v. United States*, available [here](#).

<sup>29</sup> States Department of the Treasury, *The Treasury 2021 Sanctions Review*, p.4, Oct. 2021, available [here](#).

<sup>30</sup> United States Department of the Treasury, *Enhancing the US-UK Partnership*, Oct. 17, 2022, available [here](#).

---

## **U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts**

UK and EU continue to strengthen their own sanctions regimes. Companies will need to exercise additional diligence and caution in order to ensure that they are in compliance with all applicable sanctions jurisdictions.

Additionally, we expect that the United States will continue to deploy export controls as a means of supporting sanctions programs and addressing potential national security concerns. The successful use of export controls (imposed in coordination with sanctions) to impair the Russian war effort and the novel use of export controls to target Chinese ascendancy in critical technologies deemed key to U.S. national security are models for the role export controls can play in foreign policy. Because targeted export controls may not always correspond with OFAC sanctions lists, and such controls may also be imposed countrywide, companies should ensure that their activities comply with both U.S. sanctions and export controls when entering into transactions in high-risk jurisdictions such as Russia and China.

---

## U.S. Sanctions and Export Controls 2022 Year in Review: Economic Tools Take Center Stage in Response to Global Conflicts

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

---

**David Mortlock**

202 303 1136  
dmortlock@willkie.com

**Britt Mosman**

202 303 1057  
bmosman@willkie.com

**Michael J. Gottlieb**

202 303 1442  
mgottlieb@willkie.com

**William J. Stellmach**

202 303 1130  
wstellmach@willkie.com

**Joshua Nelson**

202 303 1045  
jnelson@willkie.com

**Martin J. Weinstein**

202 303 1122  
mweinstein@willkie.com

**Peter Burrell**

44 20 3580 4702  
pburrell@willkie.com

**Grégoire Bertrou**

33 1 53 43 4579  
gbertrou@willkie.com

**Jeffrey D. Clark**

202 303 1139  
jdclark@willkie.com

**Amelia Cottrell**

212 728 8281  
acottrell@willkie.com

**Elizabeth P. Gray**

202 303 1207  
egrays@willkie.com

**Randall Jackson**

212 728 8216  
rjackson@willkie.com

**Robert J. Meyer**

202 303 1123  
rmeyer@willkie.com

**Rita D. Mitchell**

44 20 3580 4726  
rmitchell@willkie.com

**Dominique Mondoloni**

33 1 53 43 4568  
dmondoloni@willkie.com

**Simon Osborn-King**

44 20 3580 4712  
sosborn-king@willkie.com

**Dr. Richard Roeder**

49 69 7930 2364  
rroeder@willkie.com

**Michael S. Schachter**

212 728 8102  
mschachter@willkie.com

Copyright © 2023 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Frankfurt, Houston, London, Los Angeles, Milan, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at [www.willkie.com](http://www.willkie.com).