MAXINE WATERS, CA
CHAIRWOMAN

PATRICK MCHENRY, NC
RANKING MEMBER

United States House of Representatives

Committee on Financial Services

2129 Rayburn House Office Building

Washington, D.C. 20515

# Memorandum

**To:** Members, Committee on Financial Services

**From:** FSC Majority Staff

**Subject:** June 16, 2021, NSIDMP Subcommittee Hearing entitled, "Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes"

The Subcommittee on National Security, International Development, and Monetary Policy will hold a hearing entitled "Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes" on Wednesday, June 16, 2021, at 2:00 PM ET on the virtual meeting platform Cisco Webex. There will be one panel with the following witnesses:

- **Ivan A. Garces,** Principal and Chair, Risk Advisory Services, Kaufman Rossin
- **Eric B. Lorber**, Senior Director, Center on Economic and Financial Power, Foundation for Defense of Democracies
- **Lakshmi Kumar**, Policy Director, Global Financial Integrity
- **Jesse Spiro**, Global Head of Policy & Regulatory Affairs, Chainalysis
- **Dr. Jeffrey W. Taliaferro,** Professor, Department of Political Science, Tufts University

## Introduction

Economic and trade sanctions are forms of coercive statecraft that are based on "U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States."[1] A powerful non-military tool, sanctions are used to change the behavior of the target of the sanctions by limiting or eliminating access to commercial and financial markets.[2] They can be comprehensive (directed at an entire country) or targeted (narrowly scoped to a specific sector, group, entity, or individual)[3] and can be used unilaterally or multilaterally. Examples of sanctions include the blocking or freezing of a target's assets within the banking system due to engagement in the narcotics trade, prohibition on doing business with companies owned by a corrupt government official, and restrictions on the sale of certain goods and services to a targeted nation.[4] Sanctions efficacy can be improved when sanctions are part of clearly

[1] OFAC, Office of Foreign Assets Control - Sanctions Programs and Information (Last accessed 6/11/2021)
[2] Atlantic Council, Sanctions explained: How a foreign policy problem becomes a sanctions program (Sep 22, 2019)
[3] Government Accountability Office, Economic Sanctions: Agencies Assess Impacts on Targets, and Studies Suggest Several Factors Contribute to Sanctions' Effectiveness (Oct 2019)
[4] Council on Foreign Relations, What Are Economic Sanctions? (Aug 12, 2019)

defined foreign policy and national security objectives and are backed by strong alliances to both designate targets and prevent evasion.[5] In the United States, the Office of Foreign Assets Control (OFAC) at the U.S. Department of the Treasury (Treasury) administers and enforces economic and trade sanctions in partnership with the White House and other federal bodies.[6]

Given the restrictive nature of sanctions, targets of sanctions will often work to evade the sanctions' effects, sometimes with the assistance of other targets of sanctions or adversaries of the nation imposing the sanctions,[7] and thereby undermining the goals of the sanctions.[8] Sanctions evasion can give targets access to the funding or the commercial goods and services that they need to undertake the behavior that the sanctions aim to deter, such as giving terrorist groups access to funds to plan and execute attacks.

**Methods of Sanctions Evasion**

All U.S. "persons" – including U.S. citizens and permanent resident aliens regardless of location, any person or entity in the United States, and U.S. businesses and their foreign branches – must comply with OFAC prohibitions on transactions with the designated targets of sanctions.[9] Despite the breadth of that coverage, avenues for evasion are plentiful. Large, sophisticated targets like nation-states are able to leverage their control of ports, the financial sector, and national borders to provide avenues for evasion (e.g., shipping schemes),[10] and designated individuals like oligarchs or kleptocrats might employ other methods like trading in high-value art and engaging in real estate transactions.[11]

Generally, financial institutions have programs in place – using software, training, and personnel for customer onboarding and transaction monitoring – to ensure that they are complying with sanctions programs, violations of which are strict liability offenses.[12] Other businesses may not have sanctions compliance as deeply embedded into their daily operations, which is why OFAC outreach and information exchange (beyond the sanctions announcements themselves) can raise awareness of and decrease the opportunities for targets to circumvent sanctions.[13]

**Traditional Evasion**

One of the most common evasion techniques involves obscuring the true owner or beneficiary of transactions by using front or shell companies.[14] Front companies are "fully functioning company[ies] with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity," while shell companies are "incorporated compan[ies] with no independent operations, significant assets, ongoing business activities, or employees."[15] Targets of sanctions will use these legal entities to attempt to open bank accounts, purchase real estate, trade in luxury goods, and make other transactions in commercial markets (such as the purchase and movement of dual-use materials required to make weapons

[5] J W Taliaferro, Defending Frenemies: Alliance Politics and Nuclear Non-proliferation in US Foreign Policy. New York: Oxford University Press, 2019
[6] Department of State, Economic Sanctions Policy and Implementation. (last accessed Jun 6, 2021)
[7] New York Times, C Koetti, How Illicit Oil Is Smuggled Into North Korea With China's Help (Mar 24, 2021)
[8] The Guardian, North Korea defies sanctions with China's help, UN panel says (Apr 17, 2020); Treasury Press Release, Treasury Targets Sanctions Evasion Scheme Facilitating Jet Fuel Shipments to Russian Military Forces in Syria (Sep 29, 2019); Business Insider, U.S. blacklists Cuban firm tied to Venezuela sanctions evasion (Nov 26, 2019)
[9] Department of Treasury, Financial Sanctions Frequently Asked Questions (last accessed Jun 10. 2021)
[10] New York Times, E Wong, C Koettl, W Hurst, E Povoledo, Armored Cars, Robots and Coal: North Korea Defies U.S. by Evading Sanctions (Mar 9, 2020)
[11] FDD, A Erdemir, Landmark NY Trial Proves Turkish Government Complicity in Iran's Sanctions-Busting (Jan 8, 2018)
[12] Bank Policy Institute, A Bradford, Reforming the U.S. Sanctions Regulatory Regime: How a Smarter, Risk-Based Approach Can Make Sanctions More Effective (Dec 9, 2020)
[13] K2 Integrity, Navigating the Sanctions Minefield: What Every Global Business Should Know (Jun 5, 2020)
[14] FACT Coalition, How Rogue Nations & Sanctioned Groups Use Shell Companies (Feb 14, 2019)
[15] Financial Action Task Force, Concealment of Beneficial Ownership (Jul 2018)

of mass destruction). Essential to evasion methods are the incorporation, management, and facilitation services supplied to these entities and their finances by "gatekeepers," like "accountants, art advisers, bankers, corporate service providers, lawyers, luxury goods dealers, notaries, private wealth managers and real estate agents," who knowingly or unknowingly move and obscure the nature and origin of illicitly gained funds.[16] These service providers may also include professional money launderers (PMLs) who "use their occupation, business infrastructure and knowledge to facilitate money laundering activities."[17] Although there has been fierce resistance from some industries in the U.S., G7 allies such as the UK and the EU have initiated gatekeeper anti-money laundering (AML) compliance requirements.[18]

Several countries are taking steps to limit the ability of bad actors, including sanctions evaders, from abusing the financial system through legal entities. For example, both the UK and the EU have requirements for national public registries that have been established or are currently being constructed.[19] In the U.S., the 116th Congress passed the Corporate Transparency Act of 2020 (CTA, *31 U.S.C. 5336*), which similarly requires the collection of beneficial ownership of certain legal entities into a national database managed by the Financial Crimes Enforcement Network (FinCEN).[20] Although accessible only by designated government stakeholders and financial institutions with related compliance obligations, this registry increases transparency inside the U.S. for law enforcement and national security agencies seeking to understand who is hidden behind suspected illicit activity.

**Shipping Schemes**

Given the overwhelming volume of goods transported by sea, the broad reach and interconnected nature of global trade, and the sheer size of the oceans, shipping-related sanctions evasion can be highly effective. A recent bulletin released by the Department of Treasury, Department of State, and the Coast Guard detailed common shipping-related sanctions evasion methods.[21] Many of these tactics involve disguising the ship by changing the distinguishing characteristics such as its name, International Maritime Organization number, or the country flag under which it flies.[22] Ships can also obfuscate their routes by making unscheduled detours, taking an indirect route, or disabling or manipulating a ship's mandated Automatic Identification System. It is not uncommon for these actors to falsify cargo reports or to transfer cargo between ships while they are at sea. For example, recently, the Berlina, a Greek ship believed to be smuggling sanctioned Venezuelan oil, and a group of complicit ships carried out "one of the first instances of orchestrated manipulation in which vessels went dark for an extended period while off-ship agents used distant computers to transmit false locations."[23]

**Trade-Based Money Laundering**

Trade-based money laundering (TBML), like the issues in shipping, relies on the reach and breadth of global trade to transfer and legitimize proceeds from illicit ventures or sanctioned entities.[24] In practice, TBML schemes seek to create value for one side of a transaction by falsely describing goods, over- or

[16] World Economic Forum, The Role and Responsibilities of Gatekeepers in the Fight against Illicit Financial Flows: A Unifying Framework (Jun 2021)
[17] International Compliance Association, J Morris, More focus required on professional money launderers (Aug 20, 2018)
[18] Fordham Law Journal (Vol 2), D. Nougayrède, Anti-Money Laundering And Lawyer Regulation: The Response Of The Professions (Dec 2019)
[19] Schmidt & Schmidt OHG, What is the Register of Beneficial Ownership and which countries have already implemented it? (Apr 19, 2021)
[20] Ballard Spahr, P Hardy, I Babchinetskaya, K Lenahan-Pfahlert FinCEN Seeks Comments on Corporate Transparency Act Implementation (Apr 7, 2021)
[21] Department of Treasury, Department of State, and United States Coast Guard, Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities (May 14, 2020)
[22] Reuters, M Parraga, Iran uses disguised tanker to export Venezuelan oil – documents (Dec 14, 2020)
[23] Washington Post, J Goodman, Tanker's impossible voyage signals new sanction evasion ploy (May 28, 2021)
[24] CRS, L Rosen, R Miller, Trade-Based Money Laundering: Overview and Policy Issues (Jun 22, 2016)

under-invoicing, creating multiple invoices for the same shipment, or even over- or under-shipping the good itself. (See Appendix B) Through these illicit schemes, bad actors can transfer value on almost any good through the system and create what looks like legitimate cash flows.[25] In one example of this, Global Financial Integrity notes that gold "provides anonymity to organized criminals, armed groups and corrupt oligarchs alike. Furthermore, the origins of gold are exceedingly difficult to track, and without any indication whether it was produced legitimately or otherwise, gold is attractive to illicit actors wishing to hide, move or invest their illicit proceeds."[26]

**Cyber-Enabled Financial Crime**

Cybercrime, which has been used increasingly to defraud and steal funds and other valued property[27] such as data, is also being used more frequently by sanctions evaders. For example, the U.S. has attributed the criminal hacking of over a billion dollars of funds from banks, cryptocurrency exchanges, and central banks, to the Lazarus Group,[28] a military intelligence agency of the Democratic People's Republic of Korea (North Korea). Members of this organization have used a range of methods, including ATM cash-out schemes[29] and the hacking of the banks' computer networks to send fraudulent Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages.[30] Among those activities, the group is believed to be responsible for the KuCoin hack, the biggest cryptocurrency theft of 2020, amounting to$275 million worth of cryptocurrency.[31] According to the blockchain analysis firm Chainalysis, "the group is believed to have stolen more than $1.75 billion worth of cryptocurrency in the time it's been active. Experts believe proceeds from Lazarus Group hacks go toward North Korea's nuclear weapons program…"[32]

Ransomware[33] has also been used by sanctions evaders to gain access to currency. In October 2020, FinCEN[34] and OFAC[35] issued its first ransomware advisories, warning of sophisticated methods and trends in ransomware (including the sharing of exploit kits, ready-made with codes and tools, and payments made via anonymity-enhanced cryptocurrencies and mixers[36]). OFAC noted in its release that sanctions related to Russia-based "Evil Corp," the cybercriminal organization whose malware harvested login credentials from hundreds of financial institutions in over 40 countries, caused more than $100 million in theft and millions of dollars of damage to financial institutions and their customers.[37] In addition, the releases noted the risks of U.S. persons violating sanctions by making or facilitating ransom payments. Currently, it is estimated that 15% of all ransomware payments made in 2020 carried a risk of such violations.[38] As ransomware attacks continue to increase in frequency and size and where attribution is possible, more OFAC sanctions actions are possible, including against the insurance companies that increasingly indemnify against ransomware risk.[39]

---

[25] Financial Action Task Force and the Egmont Group, Trade-Based Money Laundering (Dec 2020)
[26] GFI, L Kumar, Illicit Gold in India Webinars (Dec 7, 2020)
[27] See hearing memo: Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic
[28] Also known as Reconnaissance General Bureau (RGB) and Advanced Persistent Threat 38 (APT38)
[29] Fisher & Phillips LLP, FBI Warns of Continuing Threat from "ATM Cashout" Scheme (Aug 22, 2018)
[30] Ibid.
[31] Chainalysis, Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options (Feb 9, 2020)
[32] Ibid.
[33] NECN.com, F. Bajak, Ransomware Explained: How It Works and Why Cyberattacks Are on the Rise (Jun 3, 2021)
[34] FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Oct 1, 2020)
[35] OFAC, Ransomware Advisory (Oct 1, 2020)
[36] CipherTrace, Mixers, Tumblers, Foggers (Last accessed Jun 6, 2021)
[37] OFAC, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec 5, 2019)
[38] Chainalysis, 15% of All Ransomware Payments Made in 2020 Carried a Risk of Sanctions Violations (Apr 22, 2021)
[39] BankInfoSecurity.com, D. Olenick, Should Paying Ransoms to Attackers Be Banned? (May 24, 2021)

**Virtual and Digital Assets and their Service Providers**

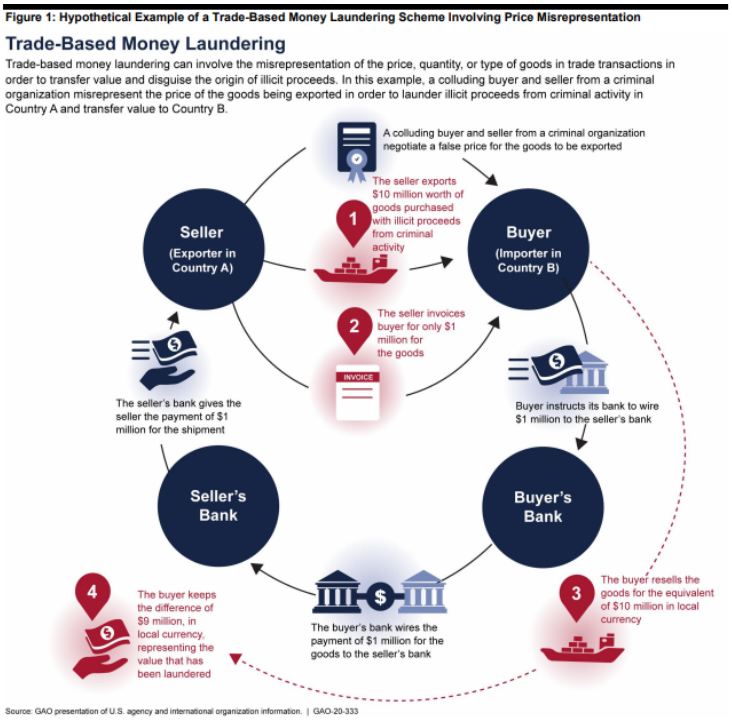
Central Bank Digital Currencies (CBDC), cryptocurrencies, and other digital assets also offer new avenues for sanctions evasion and other financial crime.[40] These assets are increasingly being used in non-transparent systems, such as decentralized exchanges (DEXs),[41] which are designed to avoid AML compliance regimes.[42] Digital currencies also present possible implications for the primacy of the U.S. dollar, which could undermine the ability of the U.S. and allies to impose effective sanctions. Although considered a failed effort, the Venezuelan petro,[43] an oil-backed cryptocurrency actively promoted by the sanctioned Nicolás Maduro government, was intended to allow sanctions targets, including the government of Venezuela, to access international financial markets and a source of currency beyond the mainstream financial system. It was for this reason that the U.S. banned transactions with the petro[44] and further sanctioned some of the entities that facilitated its development and use (See Appendix C).[45] Iran, using sanctioned oil to produce excess electricity, has built a bitcoin mining industry, encompassing 4.5% of all bitcoin mining in the world. It has, with the help of Chinese firms and others, produced approximately $1 billion a year in bitcoin, allowing it leverage other evasion tactics (such as front companies and shipping schemes) to buy imports and lessen the impact of U.S. and international sanctions.[46] As noted by the blockchain analysis and compliance firm, Elliptic, "If 4.5% of Bitcoin mining is based in Iran, then there is a 4.5% chance that any Bitcoin transaction will involve the sender paying a transaction fee to a Bitcoin miner in Iran."[47]

[40] CRS, L Rosen, R Nelson, Digital Currencies: Sanctions Evasion Risks (Feb 8, 2018)
[41] GRC World Forums, M. Rickard, DeFi brings risks and opportunities for AML (Feb 18, 2021)
[42] RUSI, K Izenman, The Other Side of the Digital Coin: Central Bank Digital Currencies and Sanctions (May 26, 2021)
[43] FDD, Fanusie et. al, To Evade U.S. Sanctions, Venezuela Launches the World's First National Cryptocurrency (Feb 23, 2018)
[44] Executive Order 13827, Taking Additional Steps to Address the Situation in Venezuela (Mar 19, 2018)
[45] Treasury, Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela (Mar 11, 2019)
[46] Elliptic, T Robinson, How Iran Uses Bitcoin Mining to Evade Sanctions & "Export" Millions of Barrels of Oil (May 21, 2021)
[47] Ibid.

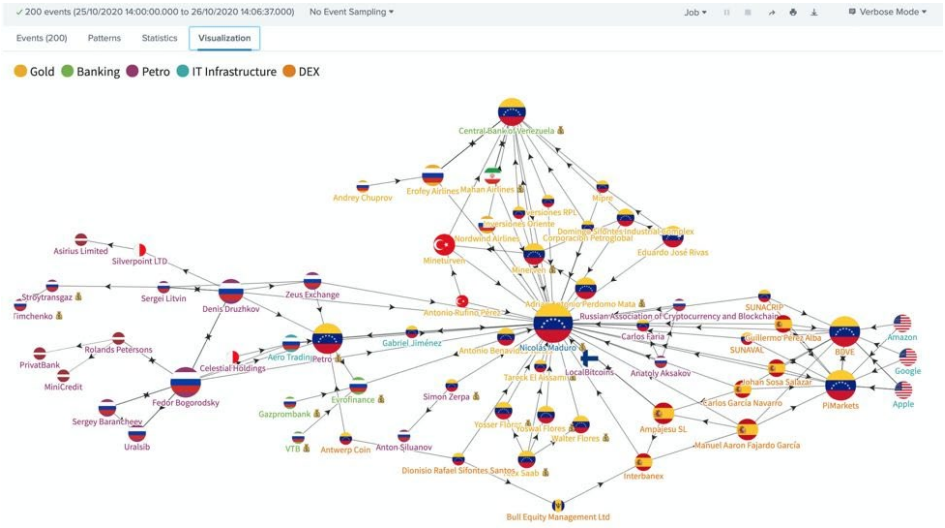
**Appendix A: Legislation**

1. **H.Res. ___,** Expressing the sense of the House of Representatives that the Under Secretary of Terrorism Finance and Intelligence or a Treasury official in a senior financial role be included in the Deputies Committee of the National Security Council.
2. **H.R. ___, Examiner Delegation Bill Act,** would require the Government Accountability Office (GAO) to study the efficacy and resourcing of the delegation of FinCEN Bank Secrecy Act (BSA) examination authority to other agencies.
3. **H.R. ___, OFAC Exchange Act,** would mandate the establishment of an OFAC outreach program, similar to the FinCEN Exchange. The outreach program would be designed to better connect with those who must comply with OFAC sanctions programs, including the financial services industry and other industries, which could benefit from increased awareness of OFAC prohibitions and processes.
4. **H.R. ___, the Combatting Illicit Finance Public-Private Partnerships Act,** would expand a section of the Anti-Money Laundering Act of 2020 to require a supervisory team of relevant federal agencies to meet periodically to advise on strategies to combat sanctions evasion.
5. **H.R. ___, OFAC Fusion Center Act,** would establish an interagency fusion center at OFAC to allow Treasury, the Department of State, the Department of Defense, and other agencies to share resources, expertise, and information in order to detect sanctions evasion efforts.
6. **H.R. ___, Money Mule Education Act,** would direct the federal financial regulators to work with financial institutions to create a program that educates consumers on the dangers and indicators of recruitment schemes, sometimes used to facilitate cyber-enabled financial crime, where an individual knowingly or unknowingly transfers illegally acquired funds on behalf on another.

## Appendix B: Hypothetical Example of a TBML Scheme Involving Price Misrepresentation[48]




## Appendix C: Entities contributing to the conservation of the Maduro regime[49]




[48] GAO, Trade--Based Money Laundering: U.S. Government Has Worked with Partners to Combat the Threat, but Could Strengthen Its Efforts (Apr 2020)

[49] Hackernoon, A Zarinski, Venezuela is Patient Zero Challenging The Western Financial System with Bitcoin (Jan 1, 2021)