SCHEMES AND SUBVERSION: HOW BAD ACTORS AND FOREIGN GOVERNMENTS UNDERMINE AND EVADE SANCTIONS REGIMES

VIRTUAL HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY

OF THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 16, 2021

Printed for the use of the Committee on Financial Services

Serial No. 117–32

U.S. GOVERNMENT PUBLISHING OFFICE
45–357 PDF WASHINGTON : 2021

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
ALMA ADAMS, North Carolina
RASHIDA TLAIB, Michigan
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
NIKEMA WILLIAMS, Georgia
JAKE AUCHINCLOSS, Massachusetts

PATRICK MCHENRY, North Carolina, *Ranking Member*
FRANK D. LUCAS, Oklahoma
PETE SESSIONS, Texas
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas

CHARLA OUERTATANI, *Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT AND MONETARY POLICY

JIM A. HIMES, Connecticut, *Chairman*

JOSH GOTTHEIMER, New Jersey
MICHAEL SAN NICOLAS, Guam
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
JAKE AUCHINCLOSS, Massachusetts

ANDY BARR, Kentucky, *Ranking Member*
PETE SESSIONS, Texas
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
LEE M. ZELDIN, New York
TOM EMMER, Minnesota
WARREN DAVIDSON, Ohio
ANTHONY GONZALEZ, Ohio

CONTENTS

WITNESSES

WEDNESDAY, JUNE 16, 2021

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

SCHEMES AND SUBVERSION: HOW BAD ACTORS AND FOREIGN GOVERNMENTS UNDERMINE AND EVADE SANCTIONS REGIMES

Wednesday, June 16, 2021

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:03 p.m., via Webex, Hon. Jim A. Himes [chairman of the subcommittee] presiding.

Members present: Representatives Himes, Gottheimer, Lynch, Dean, Auchincloss; Barr, Williams of Texas, Hill, Davidson, and Gonzalez of Ohio.

Chairman HIMES. The Subcommittee on National Security, International Development and Monetary Policy will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

Also, without objection, members of the full Financial Services Committee who are not members of this subcommittee are authorized to participate in today's hearing.

And as a reminder, I ask all Members to keep themselves muted when they are not being recognized by the Chair. The staff has been instructed not to mute Members, except when a member is not being recognized by the Chair and there is inadvertent background noise.

Members are also reminded that they may only participate in one remote proceeding at a time. If you are participating today, please keep your camera on, and if you choose to attend a different remote proceeding, please turn your camera off.

Before we get started with the substance of the hearing, I want to welcome—those who are observing will note that we have a new ranking member on this subcommittee, my friend, Andy Barr of Kentucky. I am sorry to see French Hill go, but I have a longstanding and valuable friendship and relationship with Representative Barr. So Representative Barr, welcome. And I look forward to working with you as do the rest of the members of the subcommittee.

Today's hearing is entitled, "Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes."

I now recognize myself for 5 minutes to give an opening statement.

Sanctions are an important instrument in foreign policy, designed to be both a carrot and a stick in persuading an entity, an individual, a group, or a country to change its behavior. A step beyond traditional diplomacy, it also avoids the downsides of kinetic action. We have seen the success of our sanctions regimes in bringing the Iranians to the table, and isolating human rights violators through the global Magnitsky Act, amongst others.

Our sanctions programs can only be as impactful as they are effective. When designated entities evade our sanctions, we lose an important tool from our diplomatic toolbox increasing the likelihood that military action would be necessary to maintain international order.

Our hearing today will focus on those methods of sanctions evasion ranging from physically changing the name painted on the back of a ship, the stern of a ship, to the use of shell companies to cyber-enable crime like the ransomware attacks that have been so prevalent in the news recently.

This committee has worked to address some of these issues through the passage of the Corporate Transparency Act, authored by Chairwoman Carolyn Maloney, and the Anti-Money Laundering Act, sponsored by Chairman Emanuel Cleaver as part of the 2021 National Defense Authorization Act (NDAA). These bills give law enforcement the resources and authority to better track money launderers, including sanctions evaders, and their success will depend in large part on this body adequately funding their implementation.

In addition, the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) continue to do the extremely important work of educating market participants and putting out guidance on the newest typologies of sanctions evasion; however, serious threats to the efficacy of our sanctions programs are just on the horizon and are approaching quickly.

Although, the launch of the Venezuelan "Petro" was an unambiguous failure, widespread use of alternative financial platforms could make sanctions evasion trivially simple. And although the Federal Bureau of Investigation was able to recover a portion of the ransom paid by Colonial Pipeline, we are likely to see continued growth in ransomware attacks from sanctioned entities as a way to raise funds.

With that, I would like to, again, thank our panel of witnesses. We very much appreciate you being here and your expertise. You represent that expertise in a wide variety of issues we are here to discuss today, and I sincerely appreciate your assistance in tackling them, and I look forward to your testimony.

The Chair now recognizes the ranking member of the subcommittee, Mr. Barr, for 5 minutes for an opening statement.

Mr. BARR. Thank you, Mr. Chairman, for holding the hearing today. And thank you to our witnesses for your participation.

Before we begin, I would like to say that I am very excited to be back on the National Security, International Development and Monetary Policy Subcommittee. And I appreciate the generous words of welcome from my good friend, Jim Himes, our chairman.

And as we discussed, there is a whole lot of opportunity on this subcommittee for bipartisan work and work that is very important in the interest of our country and the national security interests of our country.

This subcommittee plays a crucial role in maintaining U.S. national security through economic channels and ensuring robust international development. China continues to pose a threat to U.S. competitiveness, and American sanctions policy is more important than ever. Additionally, the impact of monetary policies is becoming increasingly evident to the everyday consumer as increased costs are hitting their wallets.

This subcommittee plays a crucial role at the intersection of the financial system and national security, and provides meaningful oversight over the Federal Reserve's monetary policy activities. I look forward to working with members of this subcommittee on both sides of the aisle to preserve a fair international financial system and ensure that the Federal Reserve remains independent and focused on its congressionally-directed mandate.

During my time on this subcommittee in previous Congresses, including as its chairman, we accomplished a great deal of significant, important work. The issues we discuss on this subcommittee transcend party lines, and I look forward to working closely with Chairman Himes and all of the members on both sides of the aisle on our shared priorities.

The U.S. employs a robust sanctions program to deny adversaries the funding, logistics, and resources to conduct illicit behavior or to compel them to change misguided behaviors. Economic and trade sanctions are enforced by the Office of Foreign Asset Control and are largely effective deterrents for bad actors; however, criminals and foreign adversaries continue to evolve and adapt and are able to evade U.S. sanctions through high- and low-tech efforts alike.

It is imperative that this subcommittee understand how bad actors are currently evading sanctions and ways that we can mitigate their continued evasion in the future. That is why I am so grateful to our chairman for calling this hearing, which I believe will help serve that purpose, as each of our witnesses brings a unique and insightful expertise to the discussion.

The U.S. maintains four major sanctions programs against Iran, North Korea, Russia, and Venezuela. These sanctions are as a result of actions by those nations that are in direct conflict with U.S. national security and global economic stability. Despite the government's focus in coordination with our international partners on sanctions enforcement, our adversaries are able to skirt the restrictions put in place.

Traditional methods of sanctions evasion include trade-based money laundering, through which bad actors move money through trade transactions; illicit shipping, including altering vessel physical identifications or corrupting other internationally-mandated

identification systems; or utilizing front companies to mask the true origin and recipient of funds.

Bad actors have utilized these sanctions evasion techniques for years and have recently amplified their sanctions evasion techniques through the use of technology. As technology develops and adapts to changing threat frameworks, our adversaries change their playbooks. For example, in the early years of the widespread use of cryptocurrency, bad actors would cash out their financing on major crypto exchanges.

However, exchanges have increased their focus on regulatory compliance including anti-money laundering (AML) and Know Your Customer (KYC) requirements, and this has chased criminals out of major exchanges into unlicensed exchanges such as Russia's Hydra marketplace.

Transaction volumes at Hydra and other unlicensed exchanges have skyrocketed in recent years as criminals identified and exploited vulnerabilities. I hope this hearing will shed light on how Congress can address these and other similar challenges.

The instances of high-profile ransomware attacks, including on elements of U.S. critical infrastructure, signify the need for improved security and coordination between the private sector and the government.

In the past year alone, victims have paid nearly $350 million in cryptocurrency to satisfy the demands of hackers using ransomware. That is a 311-percent year-over-year increase. Congress and the Administration must keep pace with the changes in advances in technology as our adversaries find new ways to evade enforcement.

I look forward to hearing from our witnesses today. Again, I thank the chairman, and I look forward to working with all of my colleagues on this new assignment.

And I yield back.

Chairman HIMES. The gentleman yields back.

Today, we welcome the testimony of our distinguished witnesses: Jeffrey Taliaferro, a professor in the Department of Political Science at Tufts University; Ivan Garces, the principal and chair of risk advisory services at Kaufman Rossin; Lakshmi Kumar, the policy director at Global Financial Integrity; Jesse Spiro, the chief of government affairs at Chainalysis; and Eric Lorber, a senior director at the Center on Economic and Financial Power at the Foundation for the Defense of Democracies. A big welcome to all of our witnesses.

Witnesses are reminded that their oral testimony will be limited to 5 minutes. You should be able to see a timer on your screen that will indicate how much time you have left, and a chime will go off at the end of your time. I would ask that you be mindful of the timer, and quickly wrap up your testimony if you hear the chime, so that we can be respectful of both the witnesses' and the subcommittee members' time.

And without objection, your written statements will be made a part of the record.

With that, Professor Taliaferro, you are now recognized for 5 minutes to give an oral presentation of your testimony.

STATEMENT OF JEFFREY W. TALIAFERRO, PROFESSOR, DEPARTMENT OF POLITICAL SCIENCE, TUFTS UNIVERSITY

Mr. TALIAFERRO. Thank you, Chairman Himes and Ranking Member Barr, for the opportunity to testify this afternoon. It is a privilege to speak to this subcommittee and to be on this distinguished panel of witnesses.

Let me state at the outset that I am a scholar of international security. I am not an economist nor am I a scholar of political economy. And my scholarship and teaching focuses primarily on U.S. national security and intelligence, the grand strategies of the great powers, both past and present, alliance politics, nuclear nonproliferation, and, more recently, cybersecurity.

My fellow witnesses are more qualified to testify about the design and implementation of sanctions, about the various strategies and tools that targeted actors employ to evade and undermine them, and to offer recommendations to Congress and to the Administration so that they might craft more effective sanctions in the future. My role on this panel is to provide a broad overview of the geopolitics of the United States' use of sanctions against a variety of actors.

Sanctions have long been an important non-kinetic tool of coercive diplomacy. The Office of Foreign Assets Control notes that sanctions are based, "on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, and economy of the United States."

The primary aim of sanctions, whether unilateral or multilateral, whether comprehensive or targeted, is to induce a change in the cost-benefit calculations of the target and thus a change in the target's behavior. But as with other tools, of course, of diplomacy, including kinetic force, the use of sanctions to secure a target's compliance is inherently difficult.

My fellow witnesses will discuss some of the newer tools and technologies used to facilitate sanctions evasion, such as cryptocurrencies, central bank digital currencies, and ransomware; however, I would like to highlight how shifting geopolitical dynamics are making it more difficult for the United States to credibly threaten and enforce sanctions, while also giving targets additional means and opportunities to evade and subvert them.

Having won the Cold War and forced the crumbling Soviet Union out of the ranks of the great powers, the United States emerged as the uni-pole, the only great power left standing in 1990, 1991. And for better or worse, for 2 decades, weak systemic, that is, international constraints and the availability of opportunities to further improve its strategic position afford the United States wide latitude in the definition and in the pursuit of its foreign policy and national security objectives.

This extreme imbalance of international power, however, had several consequences which are relevant to the subject of today's subcommittee hearing.

First, the United States imposed sanctions and even waged wars against recalcitrant states such as Iraq, Syria, Libya, and Afghani-

stan, and non-state actors such as al-Qaida, and later the Islamic State, with relative impunity.

And even when confronting state adversaries against whom the use of kinetic force would have been prohibitively costly, such as North Korea and Iran, the imposition of sanctions became a preferred tool of state-crafted successive Administrations and Congresses.

Second, U.S. military command of the commons, along with American economic and technological dominance, gave various state and non-state actors an incentive to pursue asymmetric strategies, for example, the clandestine employment of cyber criminal organizations and individual hackers by the forward intelligence services of Russia, China, North Korea, and other states.

Third, this unipolar distribution of power gave targeted states and other disaffected actors an incentive to collaborate with one another to evade or subvert U.S. sanctions. And finally, as the Biden Administration's interim national security strategic guidance acknowledges, the distribution of power across the world is changing creating new threats.

The United States now faces two great power adversaries, a rising China and a declining and revanchist Russia, along with two regional power adversaries, Iran and North Korea. All four, including their respective clients and allies, will seek to evade sanctions in the future.

In this changing geopolitical landscape, it might behoove policymakers to perhaps lower their expectations about what coercive economic diplomacy alone can achieve.

Thank you, Chairman Himes, and Ranking Member Barr.

[The prepared statement of Dr. Taliaferro can be found on page 89 of the appendix.]

Chairman HIMES. Thank you, Dr. Taliaferro.

Mr. Garces, you are now recognized for 5 minutes.

STATEMENT OF IVAN A. GARCES, PRINCIPAL AND CHAIR, RISK ADVISORY SERVICES, KAUFMAN ROSSIN

Mr. GARCES. Thank you, Chairman Himes, Ranking Member Barr, and distinguished members of the subcommittee. I thank you for the opportunity to appear before you today to talk about what I see banks doing to identify, block, reject, and report transactions subject to the U.S. sanctions.

My name is Ivan Garces, and I am a principal with Kaufman Rossin, a top 100 accounting, tax, and advisory firm where I chair the firm's Risk Advisory Services practice. I am also an executive committee member of the board of the Florida International Bankers Association (FIBA), a nonprofit trade association committed to supporting the international banking community through education, certification, and advocacy.

My comments today are based on my experience assisting financial institutions and other organizations to evaluate, remediate, and optimize risk management and programs, including those related to anti-money laundering compliance and the OFAC compliance program.

Financial institutions employ an OFAC compliance program that is generally risk-based and commensurate with their OFAC risk

profile. OFAC compliance programs typically begin with the risk assessment of an institution's customer base, products and services, nature of transactions, geographic considerations, and identification of higher-risk areas of potential OFAC sanctions risk.

Based on this risk assessment, financial institutions are expected to develop and implement policies, procedures, and internal controls for complying with OFAC. Sanctioned parties typically utilize complex structures and transactions to secure their interests in the absence or omit information from transactions to avoid detection. Two common methods utilized and discussed earlier are the exploitation of trade finance transactions and the use of shell companies.

Financial institutions typically use a combination of sanctions screening and due diligence to identify potential sanction parties and activity. Financial institutions generally screen customers against the OFAC list at prejuncture. One is at account opening, as transactions occur, and periodically, as the OFAC list is updated.

At account opening, a financial institution will typically follow their account-opening procedures, which typically include procedures to comply with the customer identification program and customer due diligence program requirements, both of which are intended to enable the financial institution to form a reasonable belief as to the true identity of each customer and assess the customer's potential risk.

Financial institutions typically also screen the customer and other relevant account parties such as account signers and beneficial owners against OFAC at this time. This process can become complicated when dealing with clients presenting with complex corporate structures, particularly offshore vehicles.

Financial institutions also typically screen transactions in real time, such as wire transfers. Financial institutions generally utilize automated interdiction systems to screen transactions and relevant transaction data speed and alert the financial institution of a potential OFAC match.

For example, wire transfer information that would generally be screened would include the originator and beneficiary bank's name, and the originator and beneficiary names and addresses. Bank identifier codes, for example, and pretext fields would all be screened for potential matches.

In the case of trade finance, banks also generally screen relevant parties in the transaction, such as importers and exporters, that have vessels, shipping companies, freight companies, freight forward, agents, and brokers. This latter process, though, is often cumbersome and manually-intensive as it involves inspection of physical documents and manual screening as opposed to automated screening.

As I mentioned earlier, the OFAC sanctions list is updated periodically, and banks generally have controls in place to ensure their systems are uploaded with the most current list, and they screen their customer database on a periodic basis.

But there are challenges in complying with OFAC. Maintaining a robust compliance program requires substantial resources. Banks must invest in people, in policies, procedures, and controls, ongoing training, and automated systems to comply with OFAC. Compli-

ance programs are tested by independent parties and examined by bank regulators. However, OFAC-sanctioned screening is not foolproof, and even the most well-intentioned OFAC compliance programs may fail to detect sanctioned activity.

With an increasing number of sophisticated bad actors, and complexity of transactions, financial institutions can't be expected to connect all the dots. Sanctions compliance programs are pretty well ingrained in financial institution risk models, but evolution of sanctions compliance programs is needed in other industries susceptible to OFAC-sanctioned risks. Government outreach and efforts to enhance corporate transparency and implement a national beneficial ownership registry is a step in the right direction.

Lastly, we can benefit from increased cooperation between the public and private sectors, such as is contemplated with the proposed OFAC Exchange Act, and the Combatting Illicit Finance Public-Private Partnerships Act legislation noted for this hearing. Government should be in a position to be able to take, analyze, and interpret information received not only from financial institutions, but other industry stakeholders, and connect the dots identifying trends and relationships across the financial system.

Thank you, again, for inviting me to appear before you today. I would be happy to respond to any questions the members of this subcommittee may have.

[The prepared statement of Mr. Garces can be found on page 30 of the appendix.]

Chairman HIMES. Thank you, Mr. Garces.

Ms. Kumar, you are now recognized for 5 minutes.

STATEMENT OF LAKSHMI KUMAR, POLICY DIRECTOR, GLOBAL FINANCIAL INTEGRITY (GFI)

Ms. KUMAR. Thank you, Chairman Himes, Ranking Member Barr, and other esteemed members of the subcommittee for the opportunity today to testify on behalf of Global Financial Integrity at this hearing.

GFI has worked tirelessly over the last decade with allies both domestically and internationally to address the gaps and vulnerabilities in the global trade and financial systems that serve as a safe haven for criminal actors. The U.S. sanctions regime is expansive and currently includes more than 30 different sanctions programs. Despite the ever-increasing reach of sanctions, with evidence showing that the number of sanctioned vessels in ports rose at an annual rate of 6 percent, oil exports by Iran and Venezuela and oil imports by North Korea keep increasing every year.

Because much of the sanctions program is targeted at curtailing the ability to conduct international commerce, sanctions evasion techniques play an international game of hide-and-seek, exploiting regulatory weaknesses both in the U.S. and globally assisted by a network of gatekeepers and facilitators.

Because of this close connection to trade, it is unsurprising that a leading mechanism to evade sanctions involves the use of Trade-Based Money Laundering (TBML) techniques. TBML is the process of disguising the proceeds of crime and moving value to trade transactions. It includes techniques like falsifying the origins of a commodity of good, over-invoicing, under-invoicing, and phantom

invoicing, where no goods really move, but just money moves. TBML is particularly challenging because there are no international standards, even at the level of the Financial Task Force and little regulation internationally. It is, therefore, the perfect ally for sanctions evaders.

Unsurprisingly, some of the largest sanctions evasion schemes most recently involving Iran used TBML techniques and the Iranian government was able to pocket $100 billion by falsifying trade records.

Similarly, the Venezuelan government, to get around U.S. sanctions on its gold sector, has flown its gold all over the world, changing its origins. So, the gold is now supposedly from the Caribbean, from Colombia, from Uganda, from Dubai, really anywhere but Venezuela. This comes at a time when U.S. imports of gold during the pandemic have increased exponentially, by some measures over 600 percent.

Erasing its history in this way means that the U.S. has no way of knowing whether the gold it imports is the same gold that it is seeking to sanction. Sanctioned entities continue to look at the U.S. as a safe haven to get around sanctions and other weaknesses of the real estate sector and the investment industry.

Professionals that have helped Iran and North Korea evade sanctions, invested their lucrative commissions in real estate so the EB–5 investor program would invest in commercial real estate and buying real estate in States like Alaska. Both commercial real estate and many of the jurisdictions where these investments take place are not part of the geographic targeting or this real estate.

Similarly, vehicles like private equity, hedge funds, and venture capital funds that are exempt from carrying out customer due diligence obligations are also involved in sanctions evasion schemes. A recent FBI leak showed that London and New York hedge funds purport using a scheme to sell prohibited items from sanctioned countries to the United States.

Finally, sanctions evasion does not just exploit the gaps in regulation; it exploits the lack of resources that enforcement agencies need to detect. The "FinCEN FILES," while problematic, revealed two different sanctions evasion schemes tied to Russia and Syria that were filed as suspicious activity reports (SARs) by financial institutions, but did not necessarily receive the treatment they should have, given the resource constraints of the agency.

The way forward, therefore, is two-pronged, addressing regulatory gaps but also providing the requisite support to enforcement, supervision, and oversight agencies. Towards that end, we strongly urge four key recommendations to be considered.

First, on FinCEN, create within FinCEN a national anti-money laundering datacenter that can carry out advanced data collection and analysis, and facilitate increased public-private partnerships. On beneficial ownership, continue to prioritize the implementation and the creation of a robust beneficial ownership registry.

The sanctions evasion schemes or really any other illicit finance schemes that have stopped us is because complex legal structures and anonymous shell companies continue to remain at the heart of it, but real collection should also be extended to include other asset

classes, like collecting BUA information on real estate and art, as well as shipping vessels that are key for sanctions evasion.

Third, customer due diligence should be required for invested vices that are money towards vehicles like private equity venture capital and also for all real estate transactions.

Finally, on TBML, it is necessary that we create a relevant set of red-flag indicators in the use of TBML, highlighting the risks of free zones and vulnerable sectors like gold.

Thank you, again, for your time today, and I look forward to any questions you may have.

[The prepared statement of Ms. Kumar can be found on page 38 of the appendix.]

Chairman HIMES. Thank you, Ms. Kumar.

Mr. Spiro, you are now recognized for 5 minutes.

STATEMENT OF JESSE SPIRO, CHIEF, GOVERNMENT AFFAIRS, CHAINALYSIS

Mr. SPIRO. Thank you, Chairman Himes, Ranking Member Barr, and distinguished members of the subcommittee. Thank you for inviting me to testify before you today on this very important topic.

My name is Jesse Spiro and I am the chief of government affairs at Chainalysis. Chainalysis is the first blockchain analysis company. We provide data, software, services, and research to government agencies and companies in over 60 countries. We follow the money through human analysis, heuristics, and cutting-edge technology. Our tools have been used to successfully investigate and prosecute a number of high-profile criminal and civil cases. We have also enabled the safe growth of the legitimate cryptocurrency ecosystem.

Our private-sector customers use Chainalysis technology to comply with their regulatory obligations, to combat money laundering, and to adhere to sanctions requirements. I am honored to be here today to speak about sanctions evasion in this ecosystem.

Today, I would like to address some common misconceptions about cryptocurrency. Cryptocurrency is one way that illicit actors evade sanctions, but the vast majority of cryptocurrency transactions are legitimate. According to our analysis, in 2020 the illicit activity was just .34 percent of all transaction volume. This was a decrease from 2019, when illicit activity represented 2.1 percent of transaction volume.

In fact, the transparency and traceability provided by the public blockchain ledger used by cryptocurrency like bitcoin allows us to understand much more than in traditional financial crime investigations.

Through blockchain analytics, investigators can follow the money. Bad actors who thought they successfully evaded detection in the past now find they have left a permanent trail for law enforcement and regulators to follow. This forensic technology, coupled with good regulatory oversight, is working.

With that foundation laid, let me highlight a few examples. Through blockchain analysis, we can confirm that adversarial nations, terrorist organizations, malicious-enabled cyber actors, and transnational criminal organizations under U.S. sanctions have used cryptocurrency in an attempt to weaken the impact or fully

circumvent sanctions just as they have done through traditional banks, trade-based money laundering, and cash. Detailed examples can be found in my written testimony.

In this challenging environment, OFAC and FinCEN have both made progress in targeting these actors. FinCEN, through their Bank Secrecy Act (BSA) oversight and prescriptive crypto advisories, and OFAC, through enforcement actions and the addition of cryptocurrency wallet identifiers, two designations, has provided significant intelligence that investigators need to understand this issue and for financial institutions to properly screen for sanctions risk beyond named screening in the digital onboarding space.

Using blockchain analysis, we can see the effectiveness of including digital currency addresses in designation. Our data demonstrates that after digital currency identifiers are included, financial flows cease to these addresses, indicating a positive impact of blacklisting wallet addresses.

By adding digital currency addresses, OFAC creates awareness and adds intelligence value for investigators and the private sector due to the immutable providence of the blockchain. Additional research can identify other cyber activities related to designated actors and entities.

I would like to recommend several ways to further strengthen the current sanctions regime, including, one, encouraging collaboration and information-sharing with international partners. To date, OFAC is the only sanctioning body that has listed digital currency addresses in designation. Cryptocurrency is global and through collaboration we expect for successful investigations and seizure of funds.

Two, increasing public-private partnerships through proposed legislation like the Combatting Illicit Finance Public-Private Partnerships Act, and the proposed OFAC Exchange Act.

Three, increasing funding to OFAC to support more comprehensive targeting and designation packages.

And four, the creation of a national crypto targeting center that would enable interagency collaboration to combat the illicit use of cryptocurrencies. This organization would provide training, intelligence, and policy support, and would facilitate information-sharing across law enforcement and regulatory agencies.

In closing, I encourage you to consider the impact any potential legislation could have on technical innovation. Our adversaries have quickly embraced cryptocurrency.

Thoughtful regulation that promotes American innovation while supporting law enforcement and financial regulators will be crucial for the United States to maintain its position as leader of the global financial system.

Thank you.

[The prepared statement of Mr. Spiro can be found on page 70 of the appendix.]

Chairman HIMES. Thank you, Mr. Spiro.

Mr. Lorber, you are now recognized for 5 minutes for a summary of your oral testimony.

STATEMENT OF ERIC B. LORBER, SENIOR DIRECTOR, CENTER ON ECONOMIC AND FINANCIAL POWER, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. LORBER. Thank you, Chairman Himes, Ranking Member Barr, and distinguished members of the subcommittee. I am honored to appear before you today to discuss how bad actors and foreign governments undermine and evade sanctions regimes.

I come before this committee as an economic sanctions and compliance professional, having worked at the U.S. Department of the Treasury and advised financial institutions, corporations, and humanitarian organizations on ensuring they operate in compliance with U.S., EU, and UN sanctions obligations. While sanctions can be a powerful tool for achieving foreign policy objectives, our adversaries are continually developing strategies and tactics to blunt their impact.

These adversaries use a range of sanctions evasion techniques, many of which rely on obfuscation and opacity to surreptitiously move funds and goods across the world, frustrating the impact of U.S. sanctions. Countering these efforts is critical to ensuring that U.S. sanctions remain effective in pressuring terrorist organizations, rogue regimes, human rights abusers, and the corrupt. At its core, sanctions evasion is about hiding the identity of the sanctioned parties involved. Many companies and individuals understand that they are prohibited from conducting transactions with sanctioned persons or in sanctioned jurisdictions, and that they face significant risks for doing so.

As a result, sanctions evaders undertake substantial efforts to hide their identities and access global markets. While U.S. adversaries have developed myriad approaches for evasion, over the last few years the U.S. Government has focused on a number of key circumvention methods, including in the maritime and financial sectors, as already discussed.

One area of concern in addition is the cryptocurrency space where we have seen rogues like Iran, Venezuela, North Korea, Hamas, al-Qaida, and the Islamic State increasingly utilize crypto assets to evade sanctions. Understanding and mitigating the risks that these cryptocurrencies may pose and, in particular, innovations like decentralized finance will be important in stopping sanctions evasion.

The U.S. Government, its allies and partners, and the private sector must adopt a multilayered defense in-depth approach to effectively counter sanctions evasion. Each layer of defense decreases the chances that a terrorist organization or rogue regime can access global markets, and while each layer may not be foolproof, together, they can pose formidable obstacles.

Elements of this approach include effective intelligence collection. Key to countering sanctions evasion is the ability to detect such activity. The Treasury Department's Office of Intelligence and Analysis, along with other members of the intelligence community, as well as FinCEN should be provided with the tools necessary to identify sanctions evasion.

A legislative proposal under consideration by this committee, the OFAC Fusion Center Act, could help achieve this. This legislation would create an interagency group designed to share data and

allow for better detection and disruption of illicit networks providing the private sector with the right tools.

In recent years, Treasury has armed the private sector with information on sanctions evasion tactics and red flags that can help companies spot such evasion through a series of advisories. Combined with clearly signaling to the private sector their compliance obligations and pursuing aggressive enforcement actions against those who fail to comply, this additional information can help the private sector more effectively counter evasion. To that end, the potential creation of an OFAC exchange which mirrors the FinCEN exchange designed to help provide the private sector with information on illicit activity, red flags, and trends could be an effective way to supplement these advisories and provide additional information on sanctions evasion.

Also, identifying and tackling cryptocurrency sanction risks. Treasury has rightly been focused on the opportunities and risks presented by cryptocurrencies and certain elements of the crypto sectors, such as decentralized finance (DeFi) that may pose particular sanctions risk, in part because those products are designed not to meet traditional gatekeepers such as centralized exchanges, as Mr. Spiro discussed. These gatekeepers often understand and implement sanctions compliance programs and have served as key force multipliers of U.S. sanctions, ensuring that a wide range of individuals and companies abide by their obligations. Determining how to ensure that new crypto market players are complying with U.S. sanctions while not stifling innovation will be an important step in combating sanctions evasion and ensuring a robust crypto marketplace.

Congress, the Administration, and the private sector must all work together to help identify, disrupt, and deter sanctions evasion. While this is a challenging task, an approach that emphasizes aggressive designations, clear communication to the private sector, and efforts to ensure regulations and guidance that effectively address risks with new innovative products will best position the United States to continue to have powerful sanctions tools.

I look forward to your questions and thank you, again, for the opportunity to testify.

[The prepared statement of Mr. Lorber can be found on page 52 of the appendix.]

Chairman HIMES. Thank you, Mr. Lorber. I will now recognize myself for 5 minutes for questions. I would like to start, actually, with you, Mr. Lorber, and maybe ask Mr. Spiro to chime in here.

This subcommittee is particularly interested in understanding and evaluating cryptocurrency. You talked about it. Is there any way to quantify the amount of sanction evasion that is occurring in all of the various cryptocurrency mechanisms that are out there? Question number one.

Question number two, is there a way to get a sense for the rate at which sanction evaders are migrating to those platforms?

And then, finally, what would you recommend beyond what is in your written testimony or what would you highlight as ways of mitigating the risk of cryptocurrency used for this purpose?

Mr. LORBER. Okay. Thank you, Mr. Chairman. It is a great series of questions, and I will also turn to the other witness for his thoughts on this as well.

In terms of quantification, I do think that—in fact, Chainalysis has a recent report that they put out which suggests that the number of transactions which are illicit that use bitcoin or blockchain technology is actually fairly low percentagewise. It is in, I believe, the low 1 percent or somewhere around there. So, it is fairly small.

In terms of specific recommendations, it is interesting to think about. There are two sort of sets of recommendations that I would focus on. One relates to ensuring that things like centralized exchanges are actually developing and employing sanctions compliance programs so that they can identify and stop sanctions evasion activity that is going through those centralized exchanges and data analytic firms like Chainalysis that do that type of work.

In addition, though, there is a series or a set of types of activities that are outside the scope of what the centralized exchanges are seeing and that is where you also have a risk for sanctions evasion activity like I was mentioning with decentralized financial products. There it is going to be partly a focus on regulation, but it will also be partly focused on education to make sure that those actors who are working in those spaces understand that if they are U.S. persons, they, too, have sanctions obligations and can be held to account if they violate them.

Mr. SPIRO. Mr. Chairman, I will hop in, and I appreciate that question. In relation to specific volumes, we do produce data explicitly in relation to both illicit and implicit that we see. And in relation to sanctions, while I don't have that information directly available now, I can provide it via written testimony after conferring with my colleagues.

In relation to recommendations, I believe that my fellow witness hit the nail on the head. When we talk about this ecosystem more broadly, the choke points are these exchanges, these centralized exchanges that provide the on-ramps and off-ramps in relation to conversion. And so, these are critical in relation to any of the other kinds of activity that happens within the ecosystem.

In relation to effective investigations being able to determine via blockchain analysis and analytics when illicit activity transacts with those choke points, that is how the information behind those bad actors and individuals is obtained, and that is how successful investigations, in turn, are prosecuted.

Chairman HIMES. Thank you, Mr. Spiro.

Mr. Garces, you have noted that even with banks that have robust compliance programs, once there is a match between a customer and somebody who is on the specially designated national list, at that point it becomes very, very human and intensive figuring out what is going on and ensuring that illicit activity doesn't take place.

What can you tell us about what the barriers are to further automation, the use of artificial intelligence (AI), and what should we be doing to help in that regard?

Mr. GARCES. Thank you, Chairman Himes. That is an excellent observation and question. The challenge is that automated systems can only do so much, and what they do is detect potential matches.

It is then up to a human to investigate the particular transaction and determine whether the potential match is, in fact, a true match or perhaps a false positive.

Advances in the technology, in the screening systems is definitely needed, and I believe artificial intelligence can help in that respect. Most systems today rely on matching algorithms and fuzzy logic to determine potential matches at certain sensitivity levels.

What happens at the next level, what the human does is to collect additional information about the parties involved in the transaction to determine ultimately whether the transaction parties are a match or not. Having systems that can automate some of that process would certainly relieve some of the efforts by the banks.

Chairman HIMES. Thank you, Mr. Garces. My time has almost expired.

So with that, I will yield back the balance of my time, and recognize Ranking Member Barr for 5 minutes of questions.

Mr. BARR. Great. Thanks, Mr. Chairman. And I appreciate the testimony of all of our witnesses on how we can improve our sanctions enforcement and prevent this evasion.

I want to first ask about North Korea. Mr. Lorber, I sponsored the Otto Warmbier North Korea Nuclear Sanctions and Enforcement Act, which became law as part of the Fiscal Year 2020 National Defense Authorization Act (NDAA).

The bill imposed some of the toughest mandatory sanctions ever on North Korea, yet in your testimony you detail how North Korea continues to evade sanctions. We have heard about the way they use shipping sometimes as sanctions evasion and front companies. Given their track record, including those front companies, hacking, and other tools, how can we better shut down North Korea's efforts to obtain hard currency or otherwise evade sanctions?

Mr. LORBER. Thank you, Ranking Member Barr. It is a great question. This goes to, in many ways, what I was speaking about in both my written and oral testimony about a defense in-depth approach. Because if there is one target out there which is incredibly sophisticated when it comes to sanctions evasion, it is North Korea, because they use front shell companies, shipping, cyber attacks, so on and so forth.

In many ways, though, the best method for combating North Korea evasion activity is information provisions to financial institutions, getting financial institutions clear typologies that the North Koreans are using in order to help them identify what looks to be potential evasion activity, as well as providing information to financial institutions not just about typologies, but also about specific entities that are associated with North Korea that appear to be front or shell companies as a way to roll them up.

And I know that historically, the Treasury has done this through a series of outreach programs to financial institutions. In addition to that, there needs to be political pressure put on those who are supporting and continue to support North Korea. It is not a secret that, for example, China has created at least a permissive environment for North Korean operatives to work in the country. That was detailed, most recently, I believe in the UN DPRK panel of experts report from, I believe, it was March 2021, as well as North Korea maintains a series of financial facilitators throughout the world, in-

cluding, I believe, in Russia and China and other jurisdictions that help North Korea evade U.S. and UN sanctions. And these individuals need to be shut down, need to be targeted, and pressure needs to be put on the governments that are hosting them to kick them out of the country.

Mr. BARR. Yes. The tough part is that our sanctions bill was the secondary sanctions that applied to Chinese banks, and how effective that has been, I am not sure; providing information to Chinese banks may not be the total answer.

Mr. LORBER. I agree with that. I think that is correct. Let me clarify what I mean by providing information to banks, in many instances by providing information to U.S. and European financial institutions where the North Koreans are trying to access those institutions through, for example, Chinese banks. There have been a number of court cases which have detailed this activity.

Mr. BARR. Great. Thanks for that. And then, in terms of the effectiveness of sanctions, we have long emphasized that sanctions should ideally bring about behavioral change on the part of bad actors. The Administration is largely responsible for determining how this works and implementing the directives of Congress.

Mr. Lorber, based on your experience at Treasury, how effective are we, generally speaking, in tying our sanctions and the lifting of sanctions to clear goals and results?

Mr. LORBER. I do think we are good at it. We are much better at it certainly than we used to be. And that is something that we tried to do, and I tried to do while I was at Treasury, to clarify very clearly to sanctions targets that if you change the behavior you are engaged in, these sanctions will be lifted.

In fact, if you look back at all of the Treasury OFAC press releases that were designation activities for the last few years, you will see that language very clearly included in there. So, it is a message that we have seen and it has been followed up by action certainly during the last Administration when there were sanctions which were lifted.

For example, sanctions that were imposed on Turkey were lifted when, in our estimation, the Turks changed their activities that we found objectionable and were the reason for the sanctions being imposed in the first place.

Mr. BARR. And last question, what type of feedback does OFAC and Treasury provide to banks with respect to implementing and enforcing sanctions? And are there ways the government can do more to strengthen or improve that public-private partnership with banks?

Mr. LORBER. Yes. That is a great question. I do like the OFAC Exchange idea, which I believe this committee has taken under consideration. The idea is that OFAC would get together with a series of financial institutions to address a specific illicit issue, in this case, maybe a sanctions evasion issue.

They would pick a number of banks or insurance companies that they believe may be seen as activity or potentially have exposure to this activity and provide them with unclassified and scrubbed information to get them to harden their systems. That is the type of information, the public-private information-sharing, that I think would be particularly effective, and I think the other witnesses

may agree. I don't want to put words in their mouths, but they may agree with that approach as well.

Mr. BARR. Thank you. I yield back.

Chairman HIMES. The gentleman's time has expired. Before I recognize the gentleman from New Jersey, I need to step away for a brief meeting, so I will thank Mr. Auchincloss for assuming the gavel in my, hopefully, brief absence.

And with that, we will recognize Mr. Gottheimer for 5 minutes.

Mr. GOTTHEIMER. Thank you, Chairman Himes, and thank you to our witnesses for being here today. Just last month, the terrorist group Hamas fired thousands of rockets into Israel [inaudible] Cutting off their funding streams. The Department of the Treasury's Office of Foreign Assets Control (OFAC) works to accomplish just that. Still, we have a lot more work to do to enhance and strengthen our sanctions.

My bipartisan legislation, the Hamas International Financing Prevention Act, requires that the President submit to Congress an annual report over the next 3 years identifying entities, including foreign persons and governments, which knowingly and materially assist Hamas or the Palestinian Islamic Jihad and impose at least two or more crippling sanctions.

Mr. Spiro, in an effort to fundraise for its military operations and skirt sanctions, Hamas has reportedly received an uptick in bitcoin donations since the terrorist group's conflict with Israel last month. What do we know about the volume of cryptocurrency being solicited by groups like Hamas, and is law enforcement equipped to track and prevent these payments?

Mr. SPIRO. Congressman, I appreciate that question. It is obviously very timely. And, in short, what I can say is, we know a significant amount of information about those payments. We know volumes. It is around $140,000 or the equivalent since September of 2020. We know additionally some of the connectivity in relation to services, the services that were used in relation to those donors. And all of that information comes, again, from the power of the data, from the power of the blockchain, and the blockchain forensics.

When it comes to law enforcement, we work with both the public and private sectors, meaning they will both have access to anything that has been attributed to terrorist financing, which is the highest risk and will support directly investigations and mitigation efforts.

Mr. GOTTHEIMER. And we know that cryptocurrency is used, particularly by Hamas, in terms of [inaudible]

Mr. SPIRO. Yes. There is legacy information in relation to solicitation of donations by Hamas going back a number of years.

Mr. GOTTHEIMER. Thank you. Can you discuss the evolution for terror financing through the use of digital assets and how it may be used by illicit actors to evade terrorism-related sanctions?

Mr. SPIRO. Yes, Congressman. And I also appreciate that question. As with any other illicit activity within this ecosystem, you do see incremental growth in relation to the illicit economy as well, and as it pertains to terrorism financing, we have seen incremental adoption.

It is relatively small, or I would even posit, extremely small comparatively not only to the other activity within the ecosystem, but to the illicit activity, but we have seen instances of it.

I would cite the fact that law enforcement domestically has been capable and able to take down multiple campaigns connected to that kind of activity, utilizing blockchain forensics and their investigative capabilities, but we have seen this technology abused by a number of terrorist organizations.

Mr. GOTTHEIMER. To that point, are there other tools that we could provide you with to help stay ahead of the activity to evade sanctions?

Mr. SPIRO. Congressman, that is also a good question, and I think, from the private sector, we are continually enhancing and advancing and adopting new technologies to combat the illicit activities that we see in this ecosystem.

I think the tools should be provided and applied to the public sector to those investigators to ensure that they have the resources so that they can produce the intelligence and the information. And to Mr. Lorber's point, when that is distributed, it makes it far more difficult for the bad actors to exploit.

Mr. GOTTHEIMER. [inaudible] Ignore congressionally-mandated sanctions. For instance, despite the Iran [inaudible], many companies continue to do business with Iran with impunity. Today, China continues to buy large quantities of Iranian oil.

Mr. Lorber, how can Congress better ensure that the Executive Branch enforces existing sanctions and, in particular, addresses China's purchase of oil from Iran and Venezuela?

Mr. LORBER. Thank you, Congressman. It is a great question. One of the biggest challenges of many of our sanctions campaigns is that there are, in effect, sanction-busting countries. China comes to mind in terms of purchase of Iranian origin crude. There are ways to do it and we actually have seen China respond in certain situations, and they have responded to aggressive designation activity of Chinese companies.

The quintessential example of this is the—I think, it was the September 2019 designation of COSCO Dalian and COSCO Dalian management, the Chinese shipping companies, huge Chinese shipping companies, which were designated for transporting Iranian origin crude. They apparently stopped transporting that crude following designation and aggressive negotiations with the U.S. State Department and with the Treasury Department. So, I do think there is—

Mr. AUCHINCLOSS. [presiding]. Mr. Lorber? The gentleman's time has expired.

Mr. GOTTHEIMER. Thanks, Mr. Chairman.

Mr. AUCHINCLOSS. The Chair now recognizes the distinguished gentleman from Texas, Mr. Williams, for 5 minutes.

Mr. WILLIAMS OF TEXAS. Before I start my questions, I want to congratulate Mr. Barr on his appointment to ranking member of this subcommittee and also thank my friend, Mr. Hill, for all of his leadership through the years. I am glad we have both of you on this subcommittee, working through these important issues that are critical to the national security of our great nation.

Last week, the Biden Administration rolled back sanctions against some former senior national Iranian company officials and several companies involved in shipping and trading petrol chemical products.

I am very concerned that these actions will allow Iran an easier path to avoid sanctions and further engage in trade-based money laundering. I would much prefer President Biden continue the Trump Administration's maximum pressure campaign against the hostile regime.

So, Mr. Lorber, can you give us your thoughts on, if you think these actions by the Biden Administration open up the door for greater sanctions evasion, or do you believe we still have tools at our disposal to monitor and influence the hostile regimes' behavior?

Mr. LORBER. Thank you, Representative Williams. I do think we still have many tools at our disposal to stop Iranian sanctions evasion activity. The Iran sanctions program is one of the most comprehensive in terms of both the primary and the secondary sanctions authorities. So, there is quite a range of authorities in place to stop Iranian activity.

The bigger question is, what is this Administration's appetite for using those tools in order to stop that activity, particularly as they continue negotiations indirectly with Iranians over a potential return to the Joint Comprehensive Plan of Action (JCPOA)? And there, it is a much more open question as to whether or not the Administration will aggressively go after Iranian activity outside of the nuclear docket right now during negotiations.

Mr. WILLIAMS OF TEXAS. Okay. We have seen an increase in ransom attacks on American businesses this past year. And I have spoken with some small business startups around my district who have expressed concern that they will never be able to protect themselves if a hostile actor attempts this type of attack on their business. They see companies with entire teams of people dedicated to cybersecurity being compromised and feel hopeless if they become the next target,

Mr. Spiro, is there anything we can be doing at the Federal level to help these businesses, small businesses that may not have the resources to put towards cybersecurity or some more established companies to defend against ransomware and other cyber attacks?

Mr. SPIRO. Congressman, I appreciate that question. And, obviously, that is top of mind given some of the recent critical infrastructure attacks that we have seen via ransomware. I would say that my recommended approach to mitigating this kind of activity is twofold. The first is to improve domestic cyber hygiene because, in fact, ransomware has been occurring since 1989, in fact, in some form or fashion. But given our data and what we saw as of 2020, there has been a significant increase which I believe was cited earlier.

The other piece is disrupting the supply chain. And what I mean by that is because we have that visibility into the payments in relation to ransomware, when that information is identified, a lot of additional intelligence is born. We are able to see not only the money laundering networks, we are able to make connectivity between strains, identify the administrators and the affiliates in relation to

these attacks, as well as the procurement vehicles used in relation to things like bulletproof hosting and VPN services.

So, by collectively utilizing this kind of information, a targeted approach can be taken to arresting different components and making this kind of activity less viable for the bad actors and the ransomware operators and groups. In fact, I believe today there was a takedown in relation to a ransomware-related network wherein one of the money laundering networks was disrupted. That would be a recommendation I would make, and that comes through law enforcement.

Mr. WILLIAMS OF TEXAS. Thank you.

Banks in the private sector played a critical role in keeping hostile actors out of the financial system. As this process gets more complicated, banks are investing more and more into machine learning and automated intelligence as they try to scan for bad actors.

So my final question, Mr. Garces is, can you discuss some of the benefits or pitfalls of machine learning in trying to automate this process compared to a manual screening?

Mr. GARCES. Thank you, Representative Williams. That is a great question. There is much to gain from automation in this process. Banks are already utilizing systems to help in their monitoring of transactions, their screening of transactions for potential illicit activity.

But there is still a large human burden in the investigative process. I would encourage or I would hope that the government can continue to encourage innovation amongst the private sector in terms of its compliance programs.

Mr. AUCHINCLOSS. Mr. Garces, the gentleman's time has expired.

Mr. GARCES. Thank you.

Mr. AUCHINCLOSS. The Chair now recognizes the gentlewoman from Pennsylvania, Ms. Dean, for 5 minutes.

Ms. DEAN. I thank the Chair, and I congratulate the new ranking member. And I thank all of you who have testified before us today for your thoughtfulness in your answers.

Ms. Kumar, I would like to start with you. In your testimony, I read with interest how you discussed the role that United States real estate, especially commercial real estate, plays in sanction evasion regimes. You specifically mentioned the Geographic Targeting Order (GTO) issued by FinCEN, which I might note includes 12 metropolitan areas only, to require U.S. title insurance companies to identify natural persons behind shell companies used in all cash purchases of residential real estate.

Given the limited metropolitan list covered by the GTO, and the fact that commercial real estate is not covered, can you speak to both of those problems; number one, the limited number of metropolitan areas, my own suburban Philadelphia or Philadelphia [inaudible] And also the fact that it is residential, not commercial. Where does this fall short in terms of our regulating evasion?

Ms. KUMAR. Thank you. That is an excellent question, and it goes to sort of understanding that sanctions evasion doesn't just—the sanctions program doesn't just target big actors like Iran and North Korea. The sanctions program also targets other individuals involved in drug trafficking.

And what we see is a lot of those individuals often evade sanctions, including former officials of the Venezuelan administration. All move or hide assets and move into real estate, and the U.S. real estate market is a popular avenue.

Now, when we talk about commercial real estate, you are absolutely right in that these sort of often find an example of the Iranians owning a massive sky scraper in New York was a purchase of commercial real estate. It continues to be unrecognized. The EB–5 investor program is investments that ultimately go into commercial real estate.

Now, a lot of this is particularly complex because commercial real estate involves multiple investors. It is not as simple as a residential purchase by a homeowner. To that end, we have to sort of—what is necessary is sort of a rethink of how we are going to apply the GTO, since the title insurance agents may not be the most relevant actors.

However, to identify gatekeepers that do continue to play a critical role in sort of putting together these transactions because commercial real estate transactions always take place through legal structures. They are never in the name of an individual.

So identifying actors like lawyers, who often play a critical role in this as sort of the pressure point at which you can conduct due diligence to know who is behind these transactions, is one way forward.

You also rightly said that it only covers 12 metropolitan areas. And a lot of the evasion schemes that we often see tied to individuals, but also generally, more generally, the use of real estate. You often see an equal split between cases that occur in GTO areas versus cases that occur in non-GTO areas.

And I will say that we have a report forthcoming in the next few months that actually looks at a series of reported cases which show that over the last 5 years, the number of cases that occur in non-GTO areas is actually slightly significantly more than in GTO areas. So, there is a whole host of vulnerabilities that do need to be addressed.

Ms. DEAN. Exactly. Those vulnerabilities—we have to take a look at what are the appropriate metropolitan areas, how do we include other real estate transactions, including commercial real estate transactions, how do we make gatekeepers have accountability, responsibility in their own professional ethics?

Mr. Garces, following up on these items, how can the United States Government better communicate with the financial services industry actors and other industry gatekeepers about the risks they may encounter or the feedback on how they should be making decisions in terms of these complex transactions in order to look for sanctions evasions?

Mr. GARCES. Thank you, Representative Dean, for that question. I think FinCEN—there is a good amount of outreach that happens where FinCEN puts out, and tries to put out information in a very general form to the financial institutions, but that information can be enriched through a stronger public-private sector type of program like what was being discussed with the OPEC Exchange Act.

I think that would be very helpful. I think institutions need the information that is collected at the national level because institu-

tions only see what they see within the four walls of their organization.

Ms. DEAN. Thank you very much.

And I see my time has just about expired.

Thank you all for your important information today, and I yield back.

Mr. AUCHINCLOSS. The Chair recognizes the distinguished gentleman from Ohio, Mr. Davidson, for 5 minutes. Is Mr. Davidson available? I am not sure we have any members on right now.

The subcommittee will stand in recess subject to the call of the Chair.

[brief recess]

Chairman HIMES. Okay. The subcommittee will come to order. Again, thank you to the witnesses for your forbearance. I apologize that we are in the midst of votes.

And with that, the gentleman from Ohio, Mr. Davidson, is recognized for 5 minutes for questions.

Mr. DAVIDSON. I thank the Chair, and I thank our witnesses.

I first would ask unanimous consent to submit two articles for the record. The first is the FinCEN FILES that appeared in Buzzfeed on September 20th of last year, and the second appeared today in the Wall Street Journal titled, "Untraceable Bitcoin Is a Myth." We have supplied both of those to the committee.

Chairman HIMES. Without objection, it is so ordered.

Mr. DAVIDSON. Thank you.

Our current sanctions regime contains faulty elements that often unintentionally harm American citizens and businesses. Too often, we see bad actors evade our sanctions infrastructure through trade-based money laundering, illicit shipping or front companies in third-party countries, and numerous other ways. Thankfully, as this hearing shows, I am not alone in recognizing the need to discuss and reform our outdated systems.

This past April, it was encouraging to see the Deputy Secretary of the Treasury announce that Treasury would conduct a top to bottom review of Treasury sanctions programs. Given the failures in the current BSA, AML, KYC framework and gaps, we should understand that doubling down on the same tools of surveillance reporting and control mechanisms in our financial systems will prove inadequate. The government should stop trying to control the tool that is money in the financial system and instead focus on targeting the illicit acts and actors. We must explore an alternative approach to BSA/AML/KYC and the sanctions regime so that we can have a flexible, targeted, and effective approach.

According to the Specially Designated Nationals (SDN) list, as of yesterday, June 15th, we have 277 aircraft, 3,668 entities, 4,603 individuals, and 406 vessels. Mr. Lorber, regarding OFAC's specially designated nationals list, are individuals or entities that are added to that list regularly monitored? Is there an end goal in mind whenever OFAC designates someone or something to that list?

Mr. LORBER. Thank you. It is a great question. The end goal is twofold, or one of two: to prevent them from engaging in illicit activity, you mentioned aircrafts, so preventing those aircrafts from shuffling or sending illicit drugs to a destination; or to get the targets to actually change their behavior, so to essentially impose pos-

session restrictions on them to get them to say, this is not worth it, we are no longer going to engage in material support for terrorism, for example.

So, there are end goals that are put into place, and Treasury, OFAC does, as a matter of course, review certain designations to see if they remain current, if the companies that were designated, for example, are no longer in existence, things along those lines.

Mr. DAVIDSON. Thank you. And I just wish I had time to explore how the licensing system tries to minimize collateral damage to Americans, but due to the—it is an old law, from 1975. We haven't really updated staffing. We have increased our sanctions by a lot, and it is tedious to try to prevent collateral damage to American citizens and American companies. But I do want to highlight some things with Chainalysis, and particularly, the emphasis on cryptocurrency.

Mr. Spiro, we hear a lot about ransomware attacks. Cryptocurrency skeptics are always fast to jump on a story involving a ransomware attack whenever cryptocurrency is used for the payment. However, the facts speak for themselves, and we know that crypto does not provide an advantage to illicit actors. Chainalysis does an excellent job of making this point. Do you think some people are too easily distracted with an anti-cryptocurrency narrative?

Mr. SPIRO. Thank you, Congressman, for that question, and thank you for your efforts thus far in your time on the Hill in relation to the broader adoption and knowledge around cryptocurrency and this technology.

I think that when you look at kind of the legacy of cryptocurrency thus far, there has been continual pushback in relation to the potential threats that have been posed, and the previous ecosystem when there was less compliance, fewer regulations around this space, and less of an understanding in relation to the technology underlying it and the transparency and traceability.

In relation to ransomware, I cited previously the fact that the first ransomware attack happened in 1989, and obviously did not utilize cryptocurrency.

Mr. DAVIDSON. Thanks for that. My time has expired, but you make great points, as you will undoubtedly throughout the hearing. The United States seized over $1 billion in crypto last year, so clearly, there is a way to do it. I yield back.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Massachusetts, Mr. Auchincloss, is recognized for 5 minutes.

Mr. AUCHINCLOSS. Thank you to the Chair and to our witnesses for their thoughtful testimony and also for their patience as we work out these logistics.

I actually want to build on what my colleague, Mr. Davidson, was asking about with Know Your Customer and blockchain. Mr. Spiro, I would like to engage with you on these questions. And because there might be a few of them, I would ask with respect that you try to keep your answers relatively concise.

So, is Know Your Customer harder with blockchain for technical reasons, for political reasons, or not at all?

Mr. SPIRO. Congressman, that is a wonderful question. And in relation to it, I think that KYC, that kind of collection, is now a different challenge because we pivoted from the brick-and-mortar institution into digital finance. As such, fake identities and fraudulent identities and deepfakes are problematic. They were cited, in fact, in relation to a recent designation on second eye solutions. And those kinds of providers providing that kind of fraudulent information means that bad actors, including sanctioned actors, could circumvent those kinds of controls and exchanges.

Mr. AUCHINCLOSS. Okay. So you are saying that there are technical reasons why blockchain would be a good vector for bad actors to evade KYC. And am I right in saying that there are also political reasons why it is hard to do KYC, because states like Russia, for example, are not providing the international cooperation we need to find these actors?

Mr. SPIRO. I think in relation to the regulation in this space, that different jurisdictions are choosing to apply or not apply them. Those that have regulatory arbitrage, unclear regulation, or have chosen to ban cryptocurrency run inherent risks in that you will see illicit activities bundled into those jurisdictions.

The Financial Action Task Force conducts mutual evaluations in relation to money laundering that potentially would impact mutual evaluation if it would continue. But it is something that we have seen in different jurisdictions that have either chosen not to apply regulation to ban cryptocurrency, for example.

Mr. AUCHINCLOSS. You had also mentioned in your recommendations that getting more sanctioning bodies to list the digital currency addresses would be a major step forward. Can you speak more to that? What would be the [inaudible] of sanctioning bodies that would need to list the digital currency addresses?

And has there been any kind of progress on that front, especially with states with whom the United States does not have a good relationship right now, and where a lot of these actors are operating from?

Mr. SPIRO. I can't speak to progress with other nations or those that the U.S. may not have such cooperation with, but I do know that other sanctioning bodies like the U.N. are becoming more familiar with abuse by countries that are under sanction, for example, in relation to virtual assets. So, I can say that.

Mr. AUCHINCLOSS. Okay. I want to circle back to the first question I asked, because I am not sure I totally understood the answer to it.

If you are a criminal operating in an polity who is regulating KYC such that you did not think you had an off-ramp to do a mixed fund or to wash it out, would blockchain offer you an advantage in obfuscating your identity over a different type of currency?

Mr. SPIRO. No. I would actually posit the complete opposite, Congressman. What I would say is that the only vulnerabilities that I would address in relation to KYC are the fact that people could circumvent them. But even if they were to, if they are engaged in illicit activity that can be seen in relation to illicit crypto activity, it is going to be very difficult for them to do anything within the ecosystem.

Mr. AUCHINCLOSS. Got it. Okay. If you were the head of OFAC, what would be the next step? Or if you were able to advise Congress to take any steps that would influence OFAC's measures, what would you advise that we do?

Mr. SPIRO. I would just advise you to apply more resources to that agency specifically in relation to there are risks associated with cryptocurrency and sanctions evasion wherein they can produce more designations that include cryptocurrency wallets. Because as identifiers for the private sector, when they have access to that information, that is how they can potentially mitigate the illicit activity.

And because of the activity with cryptocurrency, when a wallet is put on that designation list, any associated activity—or within a designation, excuse me, any associated activity and legacy activity in relation to that look back can also be—

Mr. AUCHINCLOSS. It is all visible, yes. So, you are saying OFAC can build KYC for the blockchain?

I yield back my time to the Chair.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Arkansas, Mr. Hill, is recognized for 5 minutes of questions.

Mr. HILL. I thank the Chair, and I appreciate our witnesses. It is a great panel. I appreciate their patience as we go through our Constitutional duty of running back and forth to vote.

And, Mr. Lorber, I really enjoyed reading your testimony. I thought your outline of America's sanction regimes was very helpful to members, particularly new members on the committee, in terms of the different kinds of sanctions that are imposed by the Legislative and Executive Branches.

You referenced a U.N. report from March, and this is, I assume, looking back at the U.N. sanctions on North Korea. Is that correct?

Mr. LORBER. That is correct, yes. It is a 1718 committee.

Mr. HILL. And what is your view of, have we held together on this topic of the United Nations? Would it be good if the Biden Administration's new Ambassador asked for a Security Council meeting on this particular topic to assess where we are on it, or will they do that automatically, having issued that report?

Mr. LORBER. The panel of experts reports on that committee. They issue a report and brief member states. I am not sure if there is an automatic Security Council meeting to discuss it. I will say in response to your first question, though I think it is fairly evident, based on the report itself, that members of the Security Council, in particular, China and Russia, don't—at best, don't appear to be enforcing U.N. sanctions related in particular to North Korean financial facilitators that are operating in those jurisdictions.

Mr. HILL. And is that equal land-based and maritime or mostly maritime?

Mr. LORBER. It is a combination. As I mentioned before, North Korea is extremely sophisticated in how they conduct sanctions evasion. They all combine strategies. They all do maritime obfuscation along with the use of front and shell companies with foreign financial facilitators. It is oftentimes packaged into sort of one extremely complex and sophisticated evasion network.

Mr. HILL. And are we not doing an adequate job? When I say, "we," I mean the United States and other major financial jurisdictions that have good AML/BSA work. Most of these things can pass through a European or an American touching institution, for example, somehow, somewhere. Are we not doing a good enough job on the secondary punishment, secondary sanction arena with those Russian and Chinese actors?

And if so, I know we don't have much clout to get them, to punish them, but tell me where you think that your point of weakness is aside from the fact that North Korea is great at using front companies and shell players.

Mr. LORBER. Yes. I think it is two separate choke points. One choke point is the access that the North Koreans actually oftentimes try to get to the U.S. financial system. There is a kind of myth out there that they are a hermit kingdom, and they have no access to the U.S. financial system. Recent cases suggest that is actually not the case. So, providing as much information, including typologies but also very specific information that is quietly provided to U.S. and European financial institutions, can be really impactful and helpful in helping them identify activity.

But in addition to that, the second choke point is actually focused on Russia and China who continually provide assistance—or let me rephrase that. It will at least provide extremely permissive environments in which North Korean trade-based money laundering and front and shell companies can operate without penalty or fear of retribution.

Mr. HILL. I take it that the maritime aspects are really a needle in the haystack situation in terms of, I know, during the Trump Administration, as we attempted—the Treasury did a good job, I think, trying to name flag vessels and increase the heat on that. President Trump was not always on the same page with Secretary Mnuchin on that, but we deployed Coast Guard cutters to South Korean waters. But that is not really not effective, is it?

Mr. LORBER. It is effective in limited cases, but I will say one thing, that State and Treasury and the U.S. Coast Guard did do is in early 2020, they issued a global maritime sanctions advisory that was extremely detailed and long, which basically signaled to the maritime sector that have sanctions compliance obligations. And if they don't follow those through, they may be at the point where they end up with an OFAC enforcement action or designation.

And frankly, and candidly, that sent a significant chill through the maritime sector to say, hey, we actually need to do a much better job bolstering our sanctions compliance or else we are going to be in bad shape with U.S. regulatory authorities.

Mr. HILL. So, that is a potential place through the Financial Action Task Force meetings and through our work with Treasury and our colleagues. That is a place we could put more emphasis. Is that a good thought?

Mr. LORBER. Yes. I think that is right. Figuring out how financial institutions are actually working to reduce trade finance-related sanctions, evasions in—

Mr. HILL. Thank you for your testimony.

I yield back, Mr. Chairman.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Ohio, Mr. Gonzalez, is recognized for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman, and congratulations to my friend, now Ranking Member Barr. I know he is down on the House Floor, but I'm excited for him in this new role.

I want to start my questions with Mr. Spiro, and I want to talk specifically about DeFi. So, there is a sentiment and a fear that DeFi, by design, does not allow for monitoring sanctions compliance.

One, is that true? That is sort of the first question. And the second one is, if not, how can we build that capability into OFAC as more transactions move into the DeFi space?

Mr. SPIRO. Thank you for that question, Congressman. It is a very good one. And it pertains to the emerging technology that we see on top of the preexisting technology that we see in the cryptocurrency space. Admittedly, I am not a DeFi expert, but what I can say is that DeFi provides software or claims to provide software which can then be used in a peer-to-peer capacity by those users in relation to trade.

And, as such, in relation to issues of accountability or sanction screening or transaction monitoring, vulnerabilities exist. And you can see how sanctions evasion could occur outside of other kinds of sanctions-related illicit activity like extraction attacks that could be executed by hackers, for example.

I believe that DeFi, given the nature of that model, does not fall under some regulatory regimes. But the Financial Action Task Force has taken the position and said that these kinds of services are, in fact, virtual asset service providers, or has taken a position that is pending this summer, I should say, that these kinds of providers are, in fact, virtual asset service providers or exchanges and are, therefore, subject to AML/CFT controls which would include KYC, which is not currently happening in much of the space and transaction monitoring and oversight.

Mr. GONZALEZ OF OHIO. Okay. So sort of building on that, what sort of questions should we be asking of OFAC to make sure that they can, in fact, monitor sanctions via DeFi? Because the promise of DeFi—I think DeFi is a really cool concept, but obviously, it has its challenges. The promises you don't have—you don't have the central intermediary, you just go peer-to-peer? So I guess, what should we be asking OFAC to make sure they have this properly on their radar and are developing the capabilities?

Mr. SPIRO. That is a great question also, Congressman. I think in relation to the different kinds of activity from what I have heard, OFAC and certainly FinCEN, who coordinates with OFAC and other agencies within the Treasury, is studying this kind of activity, is reviewing any potential illicit activity in the space, so I do believe that is happening.

But again, in relation to what degree the focus is applied and the kind of information intelligence that is being built in relation to potential additional designations and packages is something to certainly consider because the advancement of that technology right now in DeFi is rapid.

Mr. GONZALEZ OF OHIO. It is very rapid.

Mr. Lorber, do you have any thoughts on this?

Mr. LORBER. Yes. It is a great question, Congressman. I think Mr. Spiro really spoke well to it. In my mind, to a certain extent, it is a question of education as well as a specific regulatory approach. One thing that I've seen quite a significant amount of is firms who are operating in the DeFi space, or are coming into the DeFi space, or thinking about investing in the DeFi space, don't have a sense of what their OFAC obligations are. Not that they don't know that they are U.S. persons who are subject to sanctions. They know that, but they don't necessarily know how that is operationalized or what they should be doing for screening or for KYC and how they are supposed to do it.

I do think that in addition to some regulator clarity, there is a need to go out there and do some education once that clarity is provided to make sure that everybody knows that this is what is expected of you. And if you don't do it, then there may be enforcement activity that follows.

Mr. GONZALEZ OF OHIO. Thank you for that. I think my time—well, my time is about up. Mr. Lorber, I am going to ask you one more question. Do you think we should be adding China to the list of countries that we currently sanction? And if so, how would you structure those sanctions?

Mr. LORBER. I think there are many differences we have with the Chinese and many activities they engage in which I think are where sanctions can be impactful. I would not recommend putting in place essentially a comprehensive embargo like the U.S. has on Iran and Syria and North Korea and Cuba, et cetera, on China. I think—for all sorts of different reasons—that would be a mistake. I think the targeted way—I realize the time is up. I think the targeted way that both the Trump Administration and the Biden Administration are approaching sanctions towards China is prudent right now.

Mr. GONZALEZ OF OHIO. Great. Thank you.

I yield back.

Chairman HIMES. The gentleman's time has expired. It appears that we have no further Members with questions, so I would like to thank our witnesses for their testimony today. And thank you for your patience around the vote-induced chaos.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

With that, this hearing is adjourned.

[Whereupon, at 4:02 p.m., the hearing was adjourned.]

A P P E N D I X

June 16, 2021

TESTIMONY OF

IVAN A. GARCES

PRINCIPAL & CHAIR, RISK ADVISORY SERVICES

KAUFMAN ROSSIN

before the

COMMITTEE ON FINANCIAL SERVICES

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL

DEVELOPMENT AND MONETARY POLICY

UNITED STATES HOUSE OF REPRESENTATIVES

Virtual Hearing on

"Schemes and Subversion: How Bad Actors and Foreign Governments Undermine

and Evade Sanctions Regimes"

June 16, 2021

I. Introduction

Chairman Himes, Ranking Member Barr and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today to talk about what banks are doing to identify, block, reject and report transactions subject to U.S. sanctions. My name is Ivan Garces and I am a Principal with Kaufman Rossin, a top 100 Accounting, Tax and Advisory firm, based in South Florida where I chair the Firm's Risk Advisory Services practice. I am also an Executive Committee member of the Board and Board Treasurer of the Florida International Bankers Association (FIBA), a non-profit trade association committed to supporting the international banking community through education & certification and advocacy.

My testimony today is based on my experience assisting financial institutions evaluate, remediate, and optimize risk management programs, internal controls, anti-fraud, anti-corruption, anti-money laundering and Office of Foreign Assets Control ("OFAC") compliance programs.

Banks, and those engaged in international banking activities, play an essential role in the global payment system and are key to international trade by providing banking products and financing solutions to facilitate the international purchase and shipment of goods. As the global economy has evolved and transactions have become more complex, sanctions programs have evolved and so too has the methods and techniques for evading them. Since sanctions are utilized by the U.S. to restrict or eliminate access to the U.S. financial system, it relies heavily on private sector financial institutions to detect, prevent and report violating activity.

II. Overview of OFAC Sanctions

There are currently several international sanctions in place. I am going to focus my testimony on the sanctions imposed by the Office of Foreign Assets Control ("OFAC"). OFAC is

an office of the United States Department of the Treasury, which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals.[1] OFAC's primary sanctions may comprehensively target specific countries and governments including the imposition of broad-based trade restrictions, while others may selectively target specific individuals or entities such as those on OFACs Specially Designated Nationals And Blocked Persons ("SDN") list and Foreign Sanctions Evaders List, or target individuals or entities operating in certain sectors in a specific country.

As a general rule, OFAC requires financial institutions to: (1) block accounts and other property of specified countries, entities, and individuals; (2) prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals; and (3) report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).

III. Methods Used to Evade Sanctions

Sanctioned parties typically utilize complex structures and transactions to obscure their interest in the assets or omit information from transactions to avoid detection. Two common methods utilized are the exploitation of trade finance transactions and the use of shell companies to add anonymity to transactions and obscure the identities of the sanctioned party beneficial owners.

A. Trade Finance

Problematic trade transactions generally involve a complex web of a number of parties across the globe. These transactions facilitate the movement of money by sanctioned

[1] https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information

parties who often provide inconsistent, conflicting, or false documents related to the parties involved, the goods being shipped, the jurisdictions involved, and the vessel and shipping routes used.

B. Shell Companies

Shell companies are easy to create, provide a degree of anonymity and can be used to obscure the identity of the sanctioned party who is the beneficial owner of the assets and the ultimate beneficiary of the transactions. Often, sanctioned parties store assets and/or route transactions through a network of shell companies in an attempt to avoid detection.

IV. OFAC Compliance Program

Financial institutions employ an OFAC compliance program that is generally risk-based and commensurate with their OFAC risk profile. In May 2019, OFAC published, *A Framework for OFAC Compliance Commitments*, providing organizations with a framework of the essential elements of a sanctions compliance program. The Framework lays out five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.[2]

OFAC compliance programs typically begin with a risk assessment of an institution's customer base, products & services, nature of transactions, geographic locations, and identification of higher-risk areas of potential OFAC sanctions risk. Based on risk assessment, financial institutions are expected to develop, implement, maintain, and periodically update policies, procedures and internal controls for identifying, reviewing, escalating, and resolving potential OFAC matches, as well as reporting blocked and rejected transactions to OFAC.

[2] https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf

V. OFAC Sanctions Screening

OFAC sanctions screening is utilized by financial institutions to screen customers, transactions and transaction counterparties against the OFAC list for potential matches and generally occurs at three junctures: (1) at account opening, (2) as transactions occur, and (3) periodically as the OFAC list is updated.

At account opening or onboarding, a financial institution follows account opening procedures which typically includes procedures to comply with Customer Identification Program (CIP) requirements, which are intended to enable the financial institution to form a reasonable belief as to the true identify of each customer. In an effort to improve transparency and prevent bad actors from misusing companies to further their illicit activities, the Financial Crimes Enforcement Network ("FinCEN") issued a Customer Due Diligence final rule, which became applicable in May 2018, strengthening existing customer due diligence requirements and adding a new requirement to identify and verify the identity of the beneficial owners of legal entity customers. While many banks were already identifying and verifying the identity of beneficial owners as part of their CIP/CDD processes, FinCEN's final rule codified this requirement and helped to standardize the practice in the industry.

At this stage of account opening, financial institutions typically also screen the customer and other relevant account parties (i.e., account signors, beneficial owners) against OFAC to determine that they are not onboarding a customer who is a sanctioned individual or entity at the time the account is being opened.

Financial institutions also typically screen transactions, such as wire transfers, as they occur. Financial institutions generally utilize automated interdiction systems to screen transactions

and identify and alert the financial institution of a potential OFAC match. OFAC interdiction systems typically apply matching algorithms and screen relevant transaction data fields to identify potential name or geographical matches. For example, wire transfer transaction information that would generally be screened includes originator and beneficiary names and addresses, originator bank and beneficiary bank names and addresses, Bank Identifier Codes ("BIC"), free text fields (such as information fields). In the case of trade finance transactions, banks also generally screen relevant parties to the transaction, such as importers and exporters, vessels, shipping companies, freight forwarders, agents, and brokers. Banks may also perform additional due diligence such as open-source searches on the transaction parties and monitor for payments involving third parties and transactions being routed through high-risk jurisdictions.

These systems typically generate an alert for potential OFAC matches for review by an analyst. In resolving the alert, the analyst may require additional identifying information or need to perform additional due diligence to determine whether the alert was a true match or a false positive. The analyst will determine whether the transaction was a false positive and can be released, or whether the transaction should be escalated for further action, such as further investigation, blocking, rejecting and reporting.

The OFAC sanctions list is updated periodically. It is important that OFAC interdiction systems are running the most current OFAC list in its screening. Banks generally have controls in place to ensure their systems are uploaded with the most current list and it is common practice for banks to screen their customer base when the OFAC list is updated. Many banks screen their customer database against OFAC on a regular basis.

VI. OFAC Compliance Challenges

Maintaining a robust compliance program requires substantial resources. Banks must invest in people, policies, procedures and controls, ongoing training, and automated systems to be in compliance with OFAC requirements. Compliance programs are tested by independent parties and examined by bank regulators. A June 2021 report published by LexisNexis Risk Solutions entitled, *True Cost of Financial Crime Compliance Study, Global Report*, indicated that the projected total cost of financial crime compliance in the United States was $35.2 Billion.[3] However, OFAC sanctions screening is not foolproof and even the most well-intentioned OFAC Compliance programs may fail to detect sanctioned activity. The same June 2021 LexisNexis Risk Solutions study also cited sanctions screening as a top challenge with financial crime compliance operations facing financial institutions in North America. While many banks undergo tuning and validation exercises for their OFAC systems in an effort to maximize the efficiency and effectiveness of their systems, these systems generally rely on name matching algorithms and tend to generate a large volume of false positive alerts that can require extensive manual review and resolution. Sanctions screening is largely dependent on the quality and completeness of the information available to financial institutions and there are a number of variables such as the use of common names or name variations, aliases, acronyms, special characters, altered, obscured or missing information that may escape detection.

Most importantly, in the times in which we live with an increasing number of sophisticated bad actors, financial institutions can't be expected to connect all of the dots. Efforts to enhance corporate transparency and implement a national beneficial ownership registry, such as is provided

[3] https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report

for in the Corporate Transparency Act, is a step in the right direction, but further clarification and guidance will be needed to help ensure that additional compliance risk and regulatory expectations, that won't add value to the program, are not unintentionally created for financial institutions. Broader private sector involvement is needed, as well as evolution of sanctions compliance programs in industries susceptible to OFAC sanctions risk, such the maritime industry, import/export, precious metals and digital currency. We can benefit from increased cooperation between public and private sectors. Government and law enforcement resources are required. Whether it's the information obtained in connection with identified individuals or transactions violating OFAC, Suspicious Activity Reports or even Currency Transaction Reports, financial institutions can do the groundwork and then send the information to regulators or law enforcement. Government should be in a position to connect the dots, identifying trends and relationships across the financial system, between those seeking to avoid not only sanctions but our Country's laws and regulations. Otherwise, the information gathered by the financial institutions will be for naught.

Thank you again for inviting me to appear before you today. I would be happy to respond to any questions the members of this Subcommittee may have for me.

* * * * * * * *

House Financial Services Committee
Subcommittee on National Security, International Development, and Monetary Policy

Hearing on
Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes

Wednesday, June 16, 2021 - 2:00pm
Virtual via Cisco WebEx

Statement of
Lakshmi Kumar, Policy Director
Global Financial Integrity

Chairwoman Waters, Ranking Member McHenry, distinguished members of the Subcommittee on National Security, International Development, and Monetary Policy, it is an honor and privilege to testify before you today on the critical subject of the schemes utilized by criminal actors and bad governments to evade and undermine the U.S. sanctions regime. I am immensely grateful for the invitation and the opportunity to join this esteemed panel.

The U.S. with over 30 sanctions programs[1] has an expansive sanctions regime that is utilized to target *"individuals, corporate entities (e.g., firms, political parties, or other nonstate actors such as UNITA, al-Qaeda, ISIL), sectors of an economy (e.g., aviation or arms, financial, or commodities such as oil, diamonds, or timber); or specific regions of a country (as in Darfur in western Sudan)"*.[2] Recent advisories including the May 2020, the U.S. Departments of State, the Treasury, and the U.S. Coast Guard Advisory - "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities"[3] have sought to emphatically place the compliance burden outside their purview of large financial institutions and corporations. This is also reflected in the most enforcement actions by OFAC that target industries beyond the domain of financial services. "*Of the 25 enforcement actions OFAC pursued in 2019-2020, only four involve financial institutions."*[4]

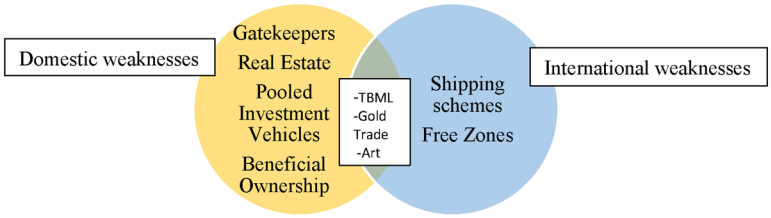
However, successful compliance of U.S. sanctions measures is predicated around an in-depth understanding of complex legal structures, sectoral understanding (how oil, gold, or timber trading works), and financial and trade arrangements. Yet actors seeking to evade and undermine U.S. sanctions exploit vulnerabilities in U.S sectors and industries that are ill-equipped to mitigate against the threats of illicit financial flows, corruption, and money laundering. Furthermore, because sanctions evasion techniques exist in a world where financial and trade networks are globally inter-connected, evasion occurs as a result of the cracks not just in the U.S. regulatory architecture but also exposes the role of - safe havens and secrecy jurisdictions[5], jurisdictions that have weak rule of law or systemic corruption[6], jurisdictions with nascent policies to target illicit finance that struggle with both technical and technological capacity, and finally the global networks of professionals that help channel money, create legal

[1] US Sanctions Programs
[2] U.S. Senate Committee on Foreign Relations, U.S.SANCTIONS POLICY IN SUB-SAHARAN AFRICA, (June 8, 2016)
[3] Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities
[4] Navigating the Sanctions Minefield: What Every Global Business Should Know (June 5, 2020)
[5] Jodi Vittori and Matthew T. Page, Dubai's Role in Facilitating Corruption and Global Illicit Financial Flows, (July 07 2020)
[6] How 7.4 Tons of Venezuela's Gold Landed in Africa—and Vanished, WSJ (June 18, 2019)

structures to obscure identity, find creative ways to hide money, all for a sizeable monetary compensation that is often re-routed back into the U.S. economy[7].

What lends further complexity to the schemes employed to evade sanctions is the complexity itself in 'how' and 'who' U.S. sanctions programs target. The 'who' reflects not only the complexity of schemes utilized to evade and undermine U.S. sanctions but also reveals the type of resources that are available to be deployed to evade sanctions.[8] Sanctions that target the critical sector of an economy[9], or an individual with a close relationship to the ruling elite[10] are harder to enforce because there will be little in the ways of checks in the home jurisdiction with the entire resources of the State and government dedicated to evading sanctions (the ports, financial institutions, law enforcement etc.). Conversely, schemes by individuals/corporate entities/ non-state organizations to evade sanctions depending on context do not automatically benefit from the vast resources of the state and rely on weak or willing governments, complicit individuals and the difficulty of enforcement and absence of adequate oversight and regulation especially in the arena of trade[11].

For the purposes of my testimony, I will discuss sectors and industries both in the U.S. and internationally where weak regulatory environments lend themselves ripe to abuse for sanctions evasion.



Use of anonymous companies and complex legal structures: The passage of the Corporate Transparency Act represented a monumental stride towards strengthening the ability of the U.S. financial system to combat illicit financial flows. The use of anonymous companies and complex corporate structures that purposefully seek to mask ownership by hiding ownership across lengthy horizontal (across multiple jurisdictions) and vertical (several layers of

[7] Lakshmi Kumar and Kaisa de Bel, Acres of Money Laundering: Why U.S. Real Estate is a Kleptocrats Dream, July 2021 (forthcoming)
[8] Iranian oil or Venezuelan oil and gold sectors
[9] 15 current, former Venezuelan officials charged with narco-terrorism, corruption, drug trafficking and other criminal charges (March 27, 2020)
[10] Tracing Sanctions Evasion Through Dubai's Luxury Real Estate Market, C4ADS (2018)
[11]

ownership) ownership chains is a consistent feature of all schemes utilized to evade sanctions.[12] This presence in nearly every sanctions evasion scheme underscores the need for FinCEN to create a strong and robust registry that can meet the national security needs of the U.S. at the earliest.

Trade related schemes: It is important to note that trade related sanctions evasion schemes are separate from TBML sanctions evasion schemes where value is transferred through the trade transaction itself. In a trade related scheme other trade related offences are used to evade sanctions. Eg. Where materials related to dual use technologies are traded between companies where the ownership is disguised to evade sanctions. This is simply a trade related scheme that utilizes anonymous or complex ownership structures, but this does not qualify as a TBML sanctions evasion scheme.

Table A. Trade related Schemes

S.No	Country	Trade related scheme
1	**Russia:** Export of illegal power turbines	After Russia's annexation of Crimea, the U.S. imposed sanctions against Russia barring the provision of goods to support Russian deep-water Arctic offshore oil projects. A Russian government-controlled business that wanted purchase a power turbine from a U.S. manufacturer utilized Russia-, Italy- and U.S.-based companies to evade the sanctions and acquire it for US$17.3 million. The true end user of the turbine was concealed from both the U.S. manufacturer and the U.S. government by submitting false documentation that stated it would be used by a U.S. company in Atlanta.

Trade Based Money Laundering: Trade based money laundering (TBML) is both a method through which to launder the proceeds of sanctions evasion but also a vital mechanism through which sanctions evasion itself takes place. According to the Financial Action Task Force (FATF), TBML is *"the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities"*.[13] Common techniques to disguise the proceeds of crime and move value through trade include misrepresenting the price, quantity, quality, type, volume, and origins of goods. This can be done through over or under invoicing, double invoicing, phantom shipments (where no good is actually moved) etc. The aim of TBML *"is not the movement of goods, but the movement of money, which the trade transactions facilitate."*[14] Another important distinction is the use of professional money launderers for TBML schemes. Professional money launders

[12] FACT Sheet: Anonymous Companies and National Security, FACT Coalition (January 2020)
[13] Trade Based Money Laundering: Trends and Developments, FATF (December 2020)
[14] Ibid

are utilized to "*take receipt of the criminal proceeds (…) and transfer or convert those proceeds, including via TBML schemes, before passing them back (…), minus the payment of their fee or commission*".[15]

Because so much of targeted U.S. sanctions is centered around the trade of commodities like oil, gold, minerals, charcoal, or dual use technologies or other restricted technologies or chemicals or precursors used in drug trafficking, there is a plethora of evidence on the use of TBML schemes to evade sanctions. Sanctions' evasion schemes tied to TBML are often meant to disguise the origins of the commodity that is being traded or the nature of the commodity itself. Unsurprisingly, the largest ever sanctions evasion scheme is a TBML scheme that allowed Iran to pocket US$100 billion and exploited both the vulnerabilities in TBML techniques but also the anonymity of the gold trade.[16]

Table B - Examples of TBML Sanctions Evasion Schemes

S.No	Country	TBML mechanism
1	**Syria:** Illegal export of laboratory equipment from the U.S. through third countries[17]	U.K. citizen Ahmed Feras Diri conspired with his brother Harold Rinko, a U.S. resident who owned an exporting firm Global Parts Supply, to ship chemical-warfare measuring equipment and other goods from the U.S. to Syria through Jordan, the U.A.E. and the U.K., without the required license. According to the indictment, they prepared false invoices that undervalued and mislabelled the goods and listed false information regarding the buyer's identity and geographic location.
2	**Venezuela:** PDVSA / oil-for-food program evasion scheme	Under the oil-for-food program (exempted from US sanctions), Mexican companies Libre Adorbo and subsidiary Schlager Business Group were used to help in the resale of Venezuelan crude oil to Asian buyers. Mexican companies claimed to have water and corn delivery contracts with government, but oil was exchanged for food at inflated prices and food was never delivered ($300 million program that did not match amount of PDVSA oil deliveries)
3	**Iran:** Billion-dollar fictitious marble businesses to evade Iranian Oil sanctions	-Kenneth Zong,a professional money launderer entered into fictious contracts with Iranian controlled companies in Iran and U.A.E. to purchase marble titles from Dubai-based tile importer and ship it to Iranian firm. He never fulfilled this role but instead submitted false contracts, invoices, bills of lading and product documentation to Korean authorities. -Zong opened bank account with Industrial Bank of Korea (IBK) for his Korean firm, through which he was paid by Iranian company for fictious service. fake invoices were used to convince IBK to release the money. -Zong converted the funds to USD and Euro, before sending wire transfers across the world to companies ultimately controlled by Iranian conspirers in service of Iranian government. Nearly all of it flowed into the UAE.

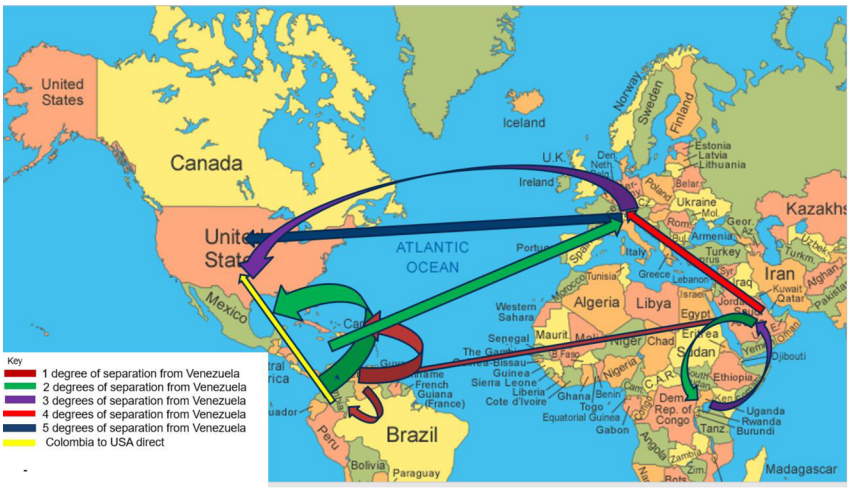
[15] Id
[16] Jonathan Schanzer, The Biggest Sanctions Evasions Scam in Recent History, The Atlantic (January 4, 2018)
[17] U.K. Man Arraigned on Conspiracy to Illegally Export Restricted Chemical Laboratory Equipment to Syria, DOJ (November 13, 2015)

Trade in Gold and other Minerals: The use and abuse of the gold trade has in the last couple of years received increased attention as a way to generate illicit finance, launder money but also to evade sanctions. The gold trade in particular is vulnerable to TBML sanctions evasion schemes because gold is easy to transport, transactions are often in cash with no paper trail, gold retains value and most importantly gold preserves anonymity. Much of the attention around the use of gold to evade sanctions has focused on schemes to mask the illicit origins of gold.[18] This is included in international sanctions efforts around limiting support to illegal armed groups in the DRC that engage in the illicit trade of natural resources including gold[19] and more recently targeted sanctions that have focused on schemes that seek to hide the origins of Venezuelan gold.

In schemes designed to hide the origins of gold, the gold is often exported from a neighboring country where its certificate of origins is falsified and once the gold is refined, it enters the larger financial systems where its problematic origins and history erased.[20] The issue of gold to evade sanctions has particularly heightened during the pandemic. Record prices of gold, coupled with the ease of anonymity that gold provides make it a perfect vehicle to garner valuable capital for sanctioned entities. U.S. imports of gold increased from $2.68 billion to $19.96 billion between 2019 to May 2020. This represented a 643.98% increase compared to the previous year.[21] At the same time, an examination of the movement of Venezuelan gold from news reports shows that to get around U.S. sanctions, Venezuelan gold has flown all over the world and quickly integrated into the international gold supply chain.[22] Other drug trafficking groups subject to U.S. sanctions like FARC have utilized the gold trade to continue their operations.[23] The ease with which illicit gold enters the legitimate market makes it nearly impossible to tell if the U.S. is importing the very gold it is trying to sanction.

Image A -The complexities of tracking Venezuelan gold[24]

[18] Lakshmi Kumar, Illicit Gold Trade: Using Trade Data and Financial Tools to Fight Money Laundering and Transnational Crime, ACFCS (July 2020)
[19] **Ibid;** UN report links Uganda to smuggled DRC gold, says exports are underdeclared, Uganda Business News (June 20, 2019)
[20] Like in the case of the DRC, where the gold is believed to move into Uganda and then gets exported as Ugandan gold.
[21] Lakshmi Kumar, Illicit Gold Trade: Using Trade Data and Financial Tools to Fight Money Laundering and Transnational Crime, ACFCS (July 2020)
[22] Ibid; Smugglers Paradise: How Venezuela is using Blood Gold to Circumvent U.S.Sanctions
[23] The Gold Standard: Addressing IFFs in the Colombian Gold Sector through Transparecny, Global Financial Integrity (February 2021)
[24] Lakshmi Kumar, Illicit Gold Trade: Using Trade Data and Financial Tools to Fight Money Laundering and Transnational Crime, ACFCS (July 2020)



Finally, the use of gold to evade sanctions is not only restricted to masking the illicit origins of gold, but as seen in the Halkbank sanctions evasion case with Iran, gold can be a critical vehicle in the layering and integration of Iranian oil proceeds into the global financial system to gain access to the U.S. dollar.[25]

Free Zones: TBML schemes are exacerbated by certain conditions and environments. Free zones provide an environment ripe for trade facilitation but that are also equally convenient for a variety of criminal behavior including sanctions evasion.

Free zones otherwise referred to as free ports, free trade zones, special economic zones and by numerous other names refers to special economic areas that benefit from tax and duties exemptions[26] and can be a way to attract business investment into a country. To attract investment into a country, free zones permit businesses to jump though regulatory hurdles quicker. These same benefits that attract legitimate businesses are equally attractive to criminal actors looking to avoid scrutiny when evading sanctions. Factors that increase the risk or likelihood of TBML include less restrictive customs environments, large amounts of paperwork, lack of data, and ports with limited regulation.[27] Free trade zones, in particular, pose a high risk for TBML because because the zones serve as pass through points for goods,

[25] Lakshmi Kumar, Illicit Gold Trade and Using Trade Data and Financial Tools, Fintelekt (October 2020); Jonathan Schanzer, The Biggest Sanctions Evasions Scam in Recent History, The Atlantic (January 4, 2018)
[26] Daniel Neale, Free Trade Zones: A Pandora's Box for Illicit Money, Global Financial Integrity (October 07, 2019)
[27] Lakshmi Kumar, Chapter 4: Dubai Free Trade or Free For All?., Carnegie Endowment (July 2020)

i.e transshipment points as opposed to ports of export and import, there is little customs presence, and little in the way of SAR reporting from free zones.

Additionally, free zones are often preferred destinations for schemes involving proliferation financing and dual use goods.[28] This is not to say that other sectors like the gold trade that are vulnerable to sanctions evasion and TBML do not use free zones. When gold moves through a free zone, as is often the case with Venezuelan gold that moves through the ABC islands or Dubai, it benefits from the additional layer of opacity that free zones provide, making the substitutions of the origins of gold an easier process.[29] Similarly, the Colon free zone in Panama is notorious as a "Mecca" for drug traffickers.[30]

"To those seeking to evade sanctions, free zones offer something else—a firewall of sorts in the paper trail linking transactions to sanctionable entities or merchandise. Though merchandise may station inside a free zone only for the few hours required to change its accompanying papers, when it departs, its place of origin is the zone itself. By allowing the repurposing of the origin of goods heading from Iran to the West and vice versa, a free zone can unwittingly help obfuscate the real entities engaged in a transaction…. When it can be found, relaxed oversight, insufficient transparency, money laundering, and illicit traffic are the ideal environment for Iranian sanctions evasion."[31]

Table C: Examples of free zones being utilized in sanctions evasion tied to Proliferation Financing and Dual Use Technologies

S. No	Examples	Nature of use	Location of Free Zone
1	German uranium enrichment components shipped illegally to Pakistan[32]	Transshipment	UAE
2	Mustard gas and nerve agent precursors shipped from India to Iran[33]		
3	Attempted export of a high-speed oscilloscope from the Netherlands to Pakistan[34]		
4	Export of maraging steel from Belgium to Iraq[35]		
5	U.S. State Department reported that TBML schemes – facilitated by the extensive number of FTZs in the UAE "might support sanctions-evasion networks and terrorist groups in Afghanistan, Pakistan, Iran, Iraq, Syria, Yemen, and Somalia.[36]		
6	Export of heavy water from Germany to India[37]		

[28] Refer to Table C
[29] Julia Yansura and Lakshmi Kumar, Narcotics Proceeds in the Western Hemisphere, Global Financial Integrity, September 2020
[30] Ibid
[31] Emanuelle Ottolanghi, "Snap-Back: A Journey Through Iranian Sanctions Evasion in Georgia," Tablet, July 1, 2015,
[32] Ibid
[33] Id
[34] Id
[35] Id
[36] U.S. Department of State, 2016 International Narcotics Control Strategy Report (INCSR), p. 220,
[37]

7	In the case of the H.Q. Khan network, FTZs in Dubai were critical in allowing nuclear technology to reach Iran, DPRK, Libya, and other states[38]		
8	In July 2020, the US Department of the Treasury published a settlement agreement with Essentra FZE, a Jebel Ali Free Zone incorporated company, which traded with and accepted payment from North Korea for the illegal export of cigarette filters using deliberately deceptive practices[39]		
9	Controlled vacuum pumps exported to Iran via a UAE-based FTZ were given a fake final destination and re-labeled and undervalued as 'spare parts'[40]		
10	Illegal export of hundreds of controlled pressure transducers from China to Iran[41]	Falsification of documentation to hide cargo	Shanghai
11	An FTZ in North-Korea, the Rason Special Economic Zone, enables Russia and China to get away with sanctions evasion due to a loophole in the sanctions that allows for the entry of goods into North Korea that are ostensibly only transiting through the country and are re-exported to third country destinations[42]	Transshipment on paper as a sanction evasion technique	North Korea
12	The Poti Free Industrial Zone (FIZ), located near to the Black Sea port city of Poti, the largest seaport in Georgia, has been used by companies seeking to evade sanctions on Iran[43]	Transshipment	Georgia

Shipping Schemes: Accounting for up to 90% of international trade, the maritime industry is also a key artery for sanction evasion. Oil exports by Iran and Venezuela and oil imports by North Korea keep increasing every year despite U.S. sanctions.[44] Moreover, the number of sanctioned vessels and ports grows with an annual rate of 6%, indicating that the use of ships in sanction evasion is becoming more prevalent.[45] At the same time, deceptive shipping methods used by bad actors are evolving and becoming more sophisticated with the aim of avoiding detection. Bad actors and rogue states involved in maritime sanction evasion often use a combination of tools aimed at concealment of the cargo, ownership or vessel location.

---

[38] Ibid at Viksi

[39] Federal Register, 'Notice of OFAC Sanctions Actions', 24 August 2020, https://www.federalregister.gov/documents/2020/08/24/2020-18527/notice-of-ofac-sanctions-actions

[40] US Department of Justice, 'Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases', June 2016, p.85, https://www.justice.gov/nsd/files/export_case_list_june_2016_2.pdf/download

[41] Viski, A. and Q. Michel (2016), "Viski, A. and Q. Michel (2016), Free Zones and Strategic Trade Controls", Strategic Trade Review, Vol. 2/3, pp. 27-41. https://strategictraderesearch.org/wp-content/uploads/2017/11/STR_03.pdf

[42] Eric Talmadge, "North Korea beating the odds despite facing toughest sanctions in decades - how?" *The Independent* (London), September 13, 2016, https://www.independent.co.uk/news/business/news/north-korea-nuclear-sanctions-china-russia-economic-trade-zone-beating-odds-a7239866.html

[43] Emanuelle Ottolanghi, "Snap-Back: A Journey Through Iranian Sanctions Evasion in Georgia," Tablet, July 1, 2015, https://www.tabletmag.com/sections/israel-middle-east/articles/iranian-sanctions-evasion

[44] https://apnews.com/article/europe-technology-business-1cd3714c9ce906b8fc931ebb95cb9e26 https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/60585d4086d5b30f0a7f1a5f/1616403804571/BLACK+GOLD.pdf ; https://www.mei.edu/publications/iranian-sanctions-evasion-and-gulfs-complex-oil-trade ; https://oilprice.com/Energy/Energy-General/Venezuela-Sees-Oil-Exports-Rise-Despite-US-Sanctions.html

[45] https://www.regulationasia.com/wp-content/downloads/RA-DowJones_Addressing_Sanctions_Risk_Maritime_Trade.pdf

Use of false flags and flag hopping: To conceal the identity or affiliation of a vessel with a sanctioned state, vessels often falsely represent the flag state that it is registered under or repeatedly change the flag state to avoid detection by authorities (i.e. flag hopping). Even after a vessel gets de-flagged, they continue to claim that flag without the consent or knowledge of that state. In those cases, bad actors often take advantage of poorly run vessel registries or states that do not have the resources to conduct proper due diligence on the vessels in their registries. There are ample reports of North Korea registering under a flag of convenience, i.e. the flag of a country other than the country of ownership, including vessels flagged in Dominica, Hong Kong, China, Panama and Sierra Leone.[46]

Obscuring ownership through complex corporate structures: Bad actors often set up complex corporate structures or frequently transfer ownership of a vessel in order to conceal the beneficial owner ultimately owning the vessel and benefitting from the shipment. To conceal beneficial ownership, bad actors are likely to use companies in jurisdiction without or with weak beneficial ownership registries. In a recent example, the U.A.E. was exposed as a hub for companies transporting Venezuelan oil.[47] Moreover, the national shipping company of Iran set up various businesses made to look like they were separate entities by registering businesses and front companies in offshore jurisdictions including the Isle of Man, Samoa, Hong Kong, Cyprus, China and Turkey. [48]

Manipulating the Automatic Identification Information System (AIS): The AIS is a satellite-based tracking system initially developed to avoid vessel collisions but is now also a useful mechanism to track vessels shipping sanctioned cargo to and from sanctioned countries. Bad actors may manipulate this signal by turning it off to conceal its location. A recent example involving a Cyprus-flagged oil tanker shows the advent of a new AIS manipulation technique. Rather than 'going dark' to conduct illicit activities, off-ship agents tampered with the AIS by leaving false tracks and making it appear as if it was in the waters near Dominica while it was really loading oil in Venezuela.[49] Although this attempt was ultimately unsuccessful because of other factors, it shows that bad actors continue to develop sanction evasion techniques to avoid detection and advances in technology.

---

[46] https://rusi.org/commentary/flagging-down-north-korea-high-seas
[47] https://www.reuters.com/article/venezuela-oil-uae-specialreport-int-idUSKBN2930YE
[48] https://sayari.com/blog/how-irans-national-shipping-company-used-offshore-companies-to-dodge-u-s-sanctions/
[49] https://apnews.com/article/europe-technology-business-1cd3714c9ce906b8fc931ebb95cb9e26

Ship-to-ship transfers and voyage irregularities: The practice of ship-to-ship transfers refers to a vessel transferring sanctioned cargo to another vessel at sea rather than at port, often 'going dark' simultaneously. The aim of this method is to hide the origin and destination of the cargo. Another method to achieve this is by taking indirect routes or making a transshipment through third countries that are not suspicious. This simultaneously gives an appearance of legitimacy, reducing the risk of detection.

U.S. Real Estate: The real estate sector has long been a preferred vehicle to evade detection and hide ill-gotten gains for a wide range of criminal actors including sanctioned governments, war criminals, kleptocrats, and drug traffickers.[50] What makes real estate valuable is the ease with which it can be used to hide the identity of the real owners and its ability to not just retain value but also create long-term profits.

The vulnerabilities of the real estate sector are not new but what is concerning is that other comparable jurisdictions like the U.K and Canada[51] that are similarly to situated to the U.S. and exposed to the same risks have in recent years taken stringent action to counter the threat of their real estate sectors being utilized as a haven for ill-gotten wealth. In the U.S. by contrast, regulatory and reporting requirements for the sector are woefully inadequate and appear to have stalled since 2018[52] and provide an easy mechanism to evade sanctions and gain access to the U.S. dollar and U.S. financial system. An often-cited example is the purchase of a New York skyscraper by the Iranian government using a series of shell companies in the U.S and in Jersey to bust through U.S. sanctions.[53] The rent from the property was ultimately routed back to Bank Melli and benefited the Iranian government. Yet current U.S. reporting requirements for the real estate sector apply only to residential real estate purchases that are all cash and purchased through a legal entity. The current Geographic Targeting Order (GTO)[54] rules would not have targeted the "commercial real estate" acquisition by the Iranian government. Similarly, the real estate sector is not just used by sanctioned entities and individuals, the sector provides a convenient way to legitimize the monies obtained by individuals that help governments like Iran and North Korea evade sanctions. In all these cases, the schemes covered U.S. States where the GTOs were not in force like Alaska or utilized the EB-5 investment program which invests in commercial real estate in the U.S. which again is not subject to the requirements of the

[50] Lakshmi Kumar and Kaisa de Bel, Acres of Money Laundering: Why U.S. Real Estate is a Kleptocrats Dream, July 2021 (forthcoming)
[51] See note 12
[52] Supra note 49
[53] Ibid
[54] FinCEN reissues Real Estate GTOs targrting 12 Metropolitain areas (April 2021)

GTOs.[55] Similarly, Venezuelan officials that were subsequently placed on sanctioned lists were able to move their ill-gotten wealth into U.S. real estate holdings with relative ease and no questions asked about their finances.[56]

Pooled Investment Vehicles: Amongst the entities that are exempt from the provision of the recently passed Corporate Transparency Act are pooled investment vehicles that include private equity, hedge funds, and venture capital funds. These entities are not required to conduct AML due diligence when accepting funds from investors. A recent leak of FBI documents revealed that these vehicles were used by drug traffickers, Russian organized crime group, and other transnational organized crime groups to move and hide their illicit finances. The leaked document cites a specific example of use in sanctions evasion schemes. In the example cited a London- and New York based hedge fund proposed "using a series of shell corporations to purchase and sell prohibited items from sanctioned countries to the United States." The proposed hedge fund was to have operated entities registered in Luxembourg and Guernsey to evade regulatory requirements when transacting with sanctioned companies.[57]

Gatekeepers: Sanctions' evasion schemes are impossible without a global network of gatekeepers and facilitators that include lawyers[58], accountants, investment advisers, art advisers[59], real estate agents, company service providers that employ their knowledge and skills to undermine the very systems their professional ethics dictate they should protect. The ability to tackle sanctions evasion is strengthened if reporting obligations exist at vulnerable points during a financial or trade transaction. Placing the burden on one singular actor like a financial institution ignores the complicit role these actors play in undermining national security, but it also presents opportunity in not creating a reporting obligation at the juncture where the vehicle, channel or scheme is created to evade U.S. sanctions. The U.S. is particularly lagging in this regard. Other G7 countries have started to require gatekeeper CDD obligations for some limited transactions. This even extends to lawyers and notaries when they are involved in real estate transactions. However, in the U.S. these requirements gatekeeper obligations continue to remain wholly absent.[60]

---

[55] https://www.justice.gov/usao-dc/pr/us-files-complaint-forfeit-500000-eb-5-visa-investment-funds-and-over-140000-sanctioned; https://www.wsj.com/articles/chinese-man-tied-to-north-korean-trade-applied-for-u-s-investment-visa-1516900647; https://www.justice.gov/opa/pr/justice-department-seeks-forfeiture-more-20-million-assets-relating-unlawful-use-us-financial

[56] https://www.nbcnews.com/news/latino/u-s-indicts-venezuelan-media-tycoon-ties-maduro-s-government-n938436

[57] https://scientologymoneyproject.com/wp-content/uploads/2020/07/FBI-Intelligence-Bulletin-Threat-Actors-Likely-Use-Private-Investment-Funds-to-Launder-Money-Circumventing-Regulatory-Tripwires2.pdf

[58] https://www.globalwitness.org/en/press-releases/undercover-investigation-american-lawyers-reveals-role-overseas-territories-moving-suspect-money-united-states/

[59] https://www.nytimes.com/2019/12/13/arts/design/art-collector-sanctions-hezbollah.html

[60] See footnote 7

The role of FinCEN: While the aim of this testimony has been to focus on the schemes used to evade sanctions, detection of those schemes through the SAR reporting mechanism falls within the purview of FinCEN. As the recent leaks of SAR filings from FinCEN revealed, the constraints around resources have meant that FinCEN is not able convert SAR reports of possible sanctions evasion into tangible enforcement action. The SARs show that Russian President Vladimir Putin's close friend Arkady Rotenberg is believed to have transferred money to Barclays Bank in London through a company called Advantage Alliance which was subsequently used to purchase vast quantities of art.[61] Similarly, these leaked files also revealed that sanctions against Syria were also likely to have been circumvented. *"The Bank of New York Mellon is reported to have transferred $224 million for a company based in Malta called Petrokim."*[62] Investigations indicated that some of the transactions possibly benefited people blacklisted under the Syrian sanctions program. Therefore, at its very crux, mitigating against sanctions evasion schemes requires adopting a two-pronged strategy: addressing the regulatory gaps in the U.S., but also strengthening the institutions responsible for supervision and oversight.

Recommendations

- **Strengthen Beneficial Ownership:**

a. FinCEN should continue to prioritize the implementation of the Corporate Transparency Act and the creation of a robust beneficial ownership registry.
b. Collecting beneficial ownership information should be extended to all legal forms and arrangements including trusts and to assets such as art, real estate, aircrafts, and boats that are owned through a foreign or domestic legal entity/ arrangement.
c. The U.S. should champion the establishment of effective beneficial ownership registries internationally including prioritizing the creation of beneficial ownership registers for states that act as 'flags of convenience'.

- **FinCEN:**

a. Ensure that FinCEN has the requisite budget necessary to meet the illicit financial flow challenges facing the U.S. trade and financial system.

---

[61] Infra
[62] https://www.dw.com/en/fincen-files-the-art-of-evading-sanctions/a-55040214

b. Create in FinCEN a National Anti-Money Laundering Data Center (NALDC) for advanced data collection, synthesis, analysis, and distribution to law enforcement for AML activity.
c. Establish a "Manhattan Project" to identify, develop and operationalize state of the art technologies needed to fulfil the technology needs of a NALDC.

- **Address Trade-based Money Laundering:**

a. Advocate for international standards to be created and implemented on TBML similar to AML/CFT. Current FATF 40 recommendations are not fit for purpose to address TBML schemes and only apply to AML.
b. Require the exchange of trade transaction information between partner countries in a mutually compatible data format. Expand this subsequently to also include the beneficial ownership information of either party to the trade transaction.
c. Conduct awareness raising and outreach programs on the vulnerabilities of TBML to sanctions evasion and create a relevant set of red flag indicators highlighting the risks of free zones and vulnerable sectors like oil, gold, dual use technologies etc.

- **Gatekeeper regulation:**

a. Real estate sector: Identify the relevant gatekeepers and extend CDD requirements to cover the purchase and sale of all real estate transactions (both commercial and residential) irrespective of value across the United States.
b. Pooled Investment vehicles: FinCEN should issue rules that require investment advisers to carry out customer due diligence including enhanced customer due diligence on all prospective investors.
c. Require gatekeeper professions including accountants, lawyers, real estate agents to meet the reporting requirements of the Bank Secrecy Act more fully. For lawyers, these CDD requirements can be limited to transactions that do not breach attorney-client privilege.

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Financial Services
Subcommittee on National Security, International Development, and Monetary Policy

Schemes and Subversion

How Targets of Sanctions Undermine and Evade Sanctions Regimes

ERIC B. LORBER

Senior Director
Center on Economic and Financial Power
Foundation for Defense of Democracies

Managing Director
K2 Integrity

Washington, DC
June 16, 2021

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

I. Introduction[1]

Chairman Himes, Ranking Member Barr, and distinguished members of the committee, I am honored to appear before you today to discuss how bad actors and foreign governments undermine and evade sanctions regimes.

I come before this committee as an economic sanctions and compliance professional, having worked at the U.S. Department of the Treasury and advised financial institutions, corporations, humanitarian organizations, and individuals on ensuring they operate in compliance with U.S., EU, and UN sanctions obligations. I have spent countless hours studying, assessing, and countering methods by which illicit actors try to evade our sanctions.

My testimony today will focus on the importance of countering sanctions evasion, which can undermine our successful use of these powerful tools of economic statecraft. Indeed, without effective efforts to counter evasion, our sanctions programs are less impactful, less likely to achieve U.S. national security objectives, and more likely to cause pain to innocents. I will provide an overview of the different types of sanctions used by the United States and then discuss the importance of countering efforts to evade these programs. I will then focus on certain key areas of sanctions evasion we have observed in the last few years, including how illicit actors have tried to circumvent our prohibitions, as well as future areas to watch. Finally, I will turn to how best to counter sanctions evasion, and what Congress, the administration, and the private sector can do to detect and disrupt evasion activity.

II. Understanding the Different Types of Sanctions

While the use of economic statecraft to achieve national security and foreign policy objectives is as old as the republic itself, over the last two decades, the United States has increasingly turned to economic sanctions and statecraft as a tool of first resort in addressing critical national security challenges.[2] Over the last four administrations, the Treasury Department, the State Department, and other executive agencies, along with Congress, have significantly increased both the number of countries and illicit actors subject to our sanctions, as well as the sophistication of these tools. In recent years, the United States has used these tools more and more. During the Trump administration, for example, the U.S. government – led by the Treasury Department's Office of Foreign Assets Control (OFAC) – designated more than 1,000 targets per year.[3]

Beyond new targets and ramped-up programs, successive administrations have imposed new and sophisticated types of sanctions to change target state behavior and prevent terrorist organizations, weapons proliferators, corrupt actors, human rights abusers, and many others from accessing the

[1] The views expressed in this testimony are my personal views and do not represent the views of the Foundation for Defense of Democracies, K2 Integrity, or the Treasury Department. Pursuant to legal and ethical obligations, I cannot discuss internal deliberations that occurred during my tenure at the Treasury Department.
[2] Juan Carlos Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York City: PublicAffairs, 2015). (https://www.publicaffairsbooks.com/titles/juan-zarate/treasurys-war/9781610391160)
[3] "2020 Year-End Sanctions Update," *Gibson Dunn*, February 5, 2020. (https://www.gibsondunn.com/wp-content/uploads/2021/02/2020-year-end-sanctions-and-export-controls-update.pdf)

international financial system. The United States now employs a range of sanctions to protect its national security interests, including:

- **Comprehensive Jurisdictional Sanctions.** Often referred to as embargoes, comprehensive sanctions prohibit U.S. persons from broadly transacting with certain countries or territories, often as a means to pressure the regime in that country. The United States currently maintains comprehensive sanctions programs on Iran, Cuba, Syria, and North Korea as well as the Crimean Peninsula.

- **Conduct/List-Based Sanctions.** List-based sanctions focus on individuals and entities engaged in illicit activity such as terrorism, weapons proliferation, drug trafficking, or malicious cyber activity, among many other illicit activities. These persons are added to the Specially Designated Nationals And Blocked Persons (SDN) List, and U.S. persons are required to block their assets. These sanctions are generally imposed to cut these persons off from legitimate financial and business markets.

- **Regime-Based Sanctions.** These are list-based sanctions that target members of current or former regimes engaged in corruption, human rights abuses, or other malign activity. These programs are not full, comprehensive programs but nevertheless target specific regimes. Examples include the U.S. sanctions programs on Libya, Burma, and Zimbabwe.

- **Sectoral Sanctions.** First employed against Russia following its annexation of Crimea and destabilizing activities in eastern Ukraine, sectoral sanctions were developed to impose costs on target companies in situations where designating those companies as SDNs was viewed as too escalatory or to have too many negative collateral consequences. Whereas SDN designations prohibit U.S. persons from engaging in any transaction with the target, sectoral sanctions prohibit *certain* transactions with the target, including prohibitions on transacting in new debt over a certain tenor or equity. The Russia sectoral sanctions program was subsequently expanded pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA). The Trump administration likewise imposed sectoral sanctions in the Venezuela program. Most recently, the Biden administration imposed sectoral sanctions on China when it issued Executive Order 14032, which prohibits U.S. persons from purchasing or selling securities of 59 Chinese companies as well as any person determined to operate in the defense or surveillance technology sectors of the Chinese economy.[4]

- **Secondary Sanctions.** Secondary sanctions extend U.S. coercive leverage to non-U.S. persons who knowingly engage in significant transactions with SDNs or in prohibited sectors (such as Iran's oil or shipping sector). Secondary sanctions authorities threaten persons who engage in such activities with being cut off from U.S. markets (including

[4] Executive Order 14032, "Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China," June 3, 2021. (https://home.treasury.gov/system/files/126/eo_cmic.pdf). For a discussion of these restrictions, see: "Biden Revises Ban on U.S. Investors Buying Certain Chinese Securities," *K2 Integrity*, June 7, 2021. (https://www.k2integrity.com/en/knowledge/policy-alerts/biden-revises-ban-on-us-investors-buying-certain-chinese-securities)

financial markets), among a number of additional penalties. Designed to pressure non-U.S. persons to cease engaging in unwanted activity with adversaries, they are often controversial with allies and partners given their so-called "extraterritorial" nature. Currently, the United States has secondary sanctions authority in the Iran, Syria, North Korea, Russia, terrorism, and Hizballah programs.

- **Non-Sanctions Economic Authorities.** In addition to sanctions, U.S. regulatory and enforcement agencies have a range of economic authorities to protect the international financial system and pressure our adversaries, including USA PATRIOT Act Section 311 identifications of institutions or jurisdictions as primary money laundering concerns; private-sector outreach and guidance through advisories issued by OFAC and Treasury's Financial Crimes Enforcement Network (FinCEN); and robust diplomacy to garner support for coordinated action with our allies and partners.

Important to note here is that these tools are not used in isolation. Congress and the executive branch frequently use overlapping authorities to target particular countries or entities. For example, the U.S. sanctions program on Russia combines a list-based program (such as Executive Orders 13660, 13661, and 14024) targeting particular Russian persons; a comprehensive jurisdictional program targeting Crimea; secondary sanctions for knowingly conducting significant financial transactions with SDNs and in certain sectors of the Russian economy; and sectoral sanctions targeting transactions in new debt or equity of certain Russian companies.

III. The Purpose of Sanctions

That these tools are used with increasing frequency should come as no surprise: They can often seem to be the best possible option from a range of suboptimal choices and can be impactful in a number of ways, including:

1. **Denying Illicit Actors Access to Global Markets and Significantly Degrading Their Capabilities.** A key objective of sanctions is to deny terrorists, human rights abusers, weapons of mass destruction (WMD) proliferators, and others access to global markets in order to make it more difficult for them to engage in malign activity. For example, successive administrations have used targeted sanctions against terrorist organizations and Islamic State leaders to degrade their capabilities and make it more difficult for them to move money and earn illicit revenue. Along with military force, the Obama and Trump administrations' efforts to constrict the Islamic State's access to the international financial system and to global markets greatly constricted the group's ability to finance its operations.[5]

2. **Imposing Economic Pain to Change Behavior.** Another key objective of sanctions policy is to compel targets to change undesirable behavior. The United States routinely uses its broad economic authorities to ramp up costs on the governments of Iran, Russia, North

[5] Assistant Secretary for Terrorist Financing Marshall Billingslea, *Testimony before House Committee on Financial Services Subcommittee on Monetary Policy and Trade*, November 30, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/sm0227.aspx)

Korea, Cuba, and Venezuela to force changes in their behavior. For example, in the Russia context, the United States has used a combination of sectoral, list-based, comprehensive jurisdictional, and secondary sanctions to impose costs on Russian President Vladimir Putin and his cronies for interfering in U.S. elections, annexing Crimea, destabilizing eastern Ukraine, supporting the Assad regime in Syria, and using chemical weapons. In the case of Iran under the Obama administration, sanctions, including those mandated by Congress, are widely credited with pressuring Iran to come to the negotiating table to discuss its nuclear program, leading to the Joint Comprehensive Plan of Action (JCPOA).

3. **Deterring Unwanted Activities.** A third key purpose of employing sanctions is deterrence. Congress and the executive branch have made clear that sanctions can serve as a key deterrent against malign activities.[6] In the case of Russia, for example, United States in April imposed sanctions and threatened further sanctions to, among other objectives, deter Moscow from engaging in additional destabilizing activities, including aggressive cyber activities and election interference.[7] While deterrence is always difficult to measure, there was some evidence to suggest that previous sanctions on Russia in 2014 did create a deterrent impact. At the time of Russia's annexation of Crimea and invasion in eastern Ukraine, it was reportedly planning on increasing the scope of its overt military support in order to wrestle key cities and territories away from Ukrainian government control, but thought twice after biting sectoral sanctions took effect.[8]

IV. The Importance of Countering Sanctions Evasion

While sanctions can be a powerful tool for achieving U.S. foreign policy objectives, our adversaries are continually developing and implementing strategies and tactics to blunt their impacts. These adversaries use a range of sanctions evasion techniques – many of which rely on obfuscation and opacity – to surreptitiously move funds and goods across the world, frustrating the impact of U.S. sanctions programs. Countering these efforts is critical to ensuring that U.S. sanctions remain effective in pressuring terrorist organizations, rogue regimes, human rights abusers, and the corrupt.

Indeed, sanctioned regimes have developed sophisticated evasion techniques that undermine the impact of economic pressure. For example, in the case of North Korea, the Kim regime has relied

---

[6] The 2015 National Security Strategy notes that U.S. "use of targeted sanctions and other coercive measures are meant not only to uphold international norms, but to deter severe threats to stability and order at the regional level." The White House, "National Security Strategy," February 2015, page 23. (https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf)

[7] "Biden Ramps Up Russia Sanctions Pressure," *K2 Integrity*, April 19, 2021. (https://www.k2integrity.com/en/knowledge/policy-alerts/biden-ramps-up-russia-sanctions-pressure)

[8] See, for example: Nigel Gould-Davies, "Sanctions on Russia Are Working: Why It's Important to Keep Up the Pressure," *Foreign Affairs*, August 22, 2018. (https://www.foreignaffairs.com/articles/russian-federation/2018-08-22/sanctions-russia-are-working). See also: Eric Lorber, "Assessing U.S Sanctions on Russia: Next Steps," *Testimony Before Senate Banking, Housing, and Urban Affairs Committee*, March 15, 2017. (https://www.banking.senate.gov/imo/media/doc/Lorber%20Testimony%203-15-17.pdf)

on a range of evasion tactics, including deceptive shipping practices, the use of front[9] and shell[10] companies to access the global financial system, and state-sponsored cyberattacks on financial institutions and cryptocurrency exchanges, to counter one of the most restrictive sanctions regimes in the world.[11] Using these multifaceted and complex evasion efforts, the regime has successfully resisted the global pressure campaign aimed at forcing Pyongyang to give up its nuclear weapons.

Detecting and disrupting sanctions evasion is often a game of cat and mouse. Financial institutions, the intelligence community, law enforcement, and others try to detect efforts by North Korea, Iran, or Hizballah to mask their true identifies through the use of front or shell companies, renamed vessels, anonymous digital assets, or a range of other methods. Oftentimes, these schemes are detected and disrupted.[12]

But sanctions evaders have certain significant advantages. First, they choose the time and place of the evasion attempt. For example, in the case of North Korea, the Kim regime has used many different front and shell companies to try and access global financial markets.[13] While certain front and shell companies are identified and shut down by law enforcement or have their efforts thwarted by financial institutions, the North Koreans can simply set up new front organizations to try to illicitly access markets using different financial institutions or different routes. In effect, the financial system and those trying to prevent sanctions evasion have to cover a wide range of possible vulnerabilities, while sanctions evaders can pick and choose how they try to infiltrate the system.

Second, and relatedly, it is often inexpensive and easy to set up evasion mechanisms. For example, establishing a front company in Singapore or Hong Kong does not require a significant investment – often just a paper registration and an address that is home to hundreds of such companies. If these front companies are engaged in illicit activity and are detected and shut down, it can be

[9] Front companies are functioning businesses that combine illicit proceeds with earnings from legitimate operations, obscuring the source, ownership, and control of the illegal funds. U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Updated Advisory on Widespread Public Corruption in Venezuela," May 3, 2019. (https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf)

[10] Shell companies are typically non-publicly traded corporations or limited liability companies that have no physical presence beyond a mailing address and generate little to no independent economic value. See: U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018. (https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf)

[11] See, for example, UN Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," S/2021/211, March 4, 2021. (https://undocs.org/S/2021/211). See also: James Byrne, Joseph Byrne, Lucas Kuo, and Lauren Sung, "Black Gold: Exposing North Korea's Oil Procurement Networks," *Royal United Services Institute and C4ADS*, 2021. (https://c4ads.org/black-gold)

[12] See, for example: U.S. Department of the Treasury, Press Release, "Treasury Targets Iran's Central Bank Governor and an Iraqi Bank Moving Millions of Dollars for IRGC-Qods Force," May 15, 2018. (https://home.treasury.gov/news/press-releases/sm0385)

[13] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)

straightforward and inexpensive to establish another front company or series of front companies in a matter of days or weeks.

V. How U.S. Adversaries Evade Our Sanctions

While U.S. adversaries have developed myriad approaches for evading sanctions, over the last few years the U.S. government has focused on a number of key circumvention methods, including in the maritime, financial, and cryptocurrency sectors. As discussed above however, even in situations where authorities generally understand the high-level of evasion risks, illicit actors are always innovating and finding new ways to get around our sanctions regimes.

At its core, sanctions evasion is about hiding the identity of the sanctioned parties involved. Many companies and individuals understand that they are prohibited from conducting transactions with sanctioned persons or in sanctioned jurisdictions and face significant risks for doing so. As a result, sanctions evaders undertake substantial efforts to hide their identities and, in doing so, are able to surreptitiously access global markets.[14]

a. Maritime Sanctions Evasion

Shipping has been described by a former senior U.S. government official as a "key artery to evade sanctions."[15] As 90 percent of global trade involves maritime transportation, sanctioned individuals and jurisdictions are constantly seeking ways to exploit the global supply chain and adapt to new restrictions.[16] As of 2019, the total value of annual world shipping trade has reached more than $14 trillion,[17] and the global commercial fleet maintains over 100,000 vessels.[18]

Since 2018, OFAC has put a spotlight on the growing use of deceptive tactics in the shipping industry by issuing maritime-related advisories, aggressively sanctioning persons in the maritime

[14] Note that this description of sanctions evasion does not include efforts by U.S. adversaries – and in some cases partners and allies – to insulate themselves from U.S. sanctions pressure. For example, following the U.S. withdrawal from participation in the JCPOA, certain European countries established the Instrument in Support of Trade Exchanges (INSTEX), a special purpose vehicle designed to facilitate trade with Iran. INSTEX was designed to create a trade channel between European countries and Iran that the United States would not sanction, but it was not an effort to evade U.S. sanctions through obfuscation or deception. Likewise, potential Chinese efforts to establish a People's Central Bank of China-backed digital currency that could serve as an international medium of exchange – thus limiting exposure to the U.S. dollar and, by extension, U.S. sanctions pressure – likewise does not rely on deception. Rather, these methods are more straightforward approaches to blunting the impact of U.S. sanctions.

[15] Jonathan Saul, "U.S. sets sights on shipping companies for sanctions evasions," *Reuters*, November 6, 2019. (https://www.reuters.com/article/us-shipping-usa-sanctions/u-s-sets-sights-on-shipping-companies-for-sanctions-evasions-idUSKBN1XG2CH)

[16] U.S. Department of Commerce, National Oceanic and Atmospheric Administration, Office for Coastal Management, "Fast Facts: Ports," accessed June 11, 2021. (https://coast.noaa.gov/states/fast-facts/ports.html)

[17] "Shipping and world trade: driving prosperity," *International Chamber of Shipping*, accessed June 11, 2021. (https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/#:~:text=For%20an%20economic%20region%20such,than%2014%20trillion%20US%20Dollars)

[18] Michael Horwitz, "Revealing risk through insights into ship-to-ship cargo transfers," *Windward*, accessed June 11, 2021. Revealing risks through insights into ship-to-ship cargo transfers, Windward. (https://www.wnwd.com/blog/identifying-risk-through-ship-to-ship-cargo-insights)

sector, and engaging with stakeholders in the maritime sector to ensure they understand their due diligence obligations.

Tactics deployed by sanctions evaders often include:

- Frequent changes to the names of vessels;
- Frequent changes to vessel ownership and management;
- Utilizing large barges and bulk-carrier vessels to reduce the number of ship-to-ship transfers;
- Disabling or manipulating a vessel's automatic identification systems (AIS);
- Ship-to-ship transfers;
- Voyage irregularities;
- False flags and flag hopping;
- Falsifying cargo and vessel documents;
- Physically altering vessel identification; and
- Complex ownership or management.

Such tactics can be seen through the well-known *Grace 1* case. In July 2019, Gibraltar authorities seized the *Grace 1*, a Panamanian-flagged oil tanker, for breaching international sanctions. The *Grace 1* was carrying 2.1 million barrels of Iranian crude oil to Syria. The vessel was impounded for 43 days, and the U.S. Department of Justice (DOJ) issued a seizure warrant and forfeiture complaint against the vessel and cargo.[19]

DOJ alleged that several front companies owned, operated, and managed the *Grace 1*, but that it was ultimately controlled by the Islamic Revolutionary Guards Corps (IRGC) and was used to conceal Iranian oil sales and transport. Between 2018 and 2019, the vessel would deactivate its AIS to load petroleum in Iranian ports and offload it in different locations, including by engaging in ship-to-ship transfers with vessels that previously engaged with Syrian ports. The complaint also described fraudulent documents and the use of multiple companies as intermediaries to obfuscate the participation of sanctioned Iranian persons and to circumvent U.S. sanctions on the Iranian energy sector. The seizure of the vessel highlighted the scope of sanctions evasion in the global shipping industry and challenges of enforcement.

As part of its efforts to disrupt sanctions evasion in the maritime sector, OFAC, along with the State Department and the Coast Guard, issued a global maritime sanctions advisory in 2020 that set compliance expectations for a range of actors operating in the shipping sector.[20] This advisory catalyzed compliance efforts in the sector, particularly by shipping companies, insurance companies, and port managers and operators, to significantly bolster their sanctions compliance programs.

---

[19] Verified Complaint for Forfeiture in Rem, *United States v. Oil Tanker – "GRACE 1" (IMO 9116412), et al.*, 1:19-cv-1989-(JEB) (D.D.C., filed August 16, 2019). (https://www.justice.gov/opa/press-release/file/1196361/download)
[20] U.S. Department of the Treasury, U.S. Department of State, and U.S. Coast Guard, Advisory, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," May 14, 2020. (https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf)

But even now we are seeing innovative methods by illicit actors in the maritime sector to evade U.S. sanctions and move illicit cargo. For example, recent vessel tracking has revealed new, anomalous behavior that suggests sanctions evaders in the maritime sector are adopting new approaches to avoid detection. For example, earlier this year, the Cyrus-flagged oil tanker *Berlina* was transmitting its location near the Caribbean island of Dominica when, according to vessel tracking information, it stopped and within two minutes turned 180 degrees (likely impossible for a ship of its size). In addition, while the vessel's transponder indicated that it was in the Caribbean, around the same time it was spotted physically loading crude oil near Venezuela. This could be representative of a new sanctions-evasion approach and could be "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."[21]

As the United States and its allies and partners aim to cut off sanctions evasion in the maritime sector, we can expect illicit actors to adopt new and sophisticated approaches to avoid these restrictions.

b. Financial Obfuscation

The U.S. dollar continues to play a large role in the global economy: About half of all international trade is invoiced in U.S. dollars. The dollar is involved in nearly 90 percent of all transactions in foreign exchange markets and comprises approximately 61 percent of global central bank reserves.[22] Even our adversaries under sanctions seek dollars to settle their transactions and need access to the U.S. financial system to settle dollar-denominated transactions. To do so, they use a number of financial obfuscation tactics and approaches to evade U.S. sanctions and access the U.S. financial system or sensitive U.S. goods. These tactics include using complex networks of businesses to layer illicit payments, with the goal of making transactions appear legitimate and obscuring the true originator, beneficiary, and purpose of the transactions. Two of our adversaries, in particular, make extensive use of these tactics: North Korea and Iran.

North Korea

North Korea relies on elaborate networks to circumvent U.S. and UN sanctions and to gain indirect access to the financial system and procure critical goods in support of its WMD program.[23] State-owned enterprises and banks use front and shell companies located abroad and a network of bank representatives and embassy personnel to conceal the true beneficiaries of transactions. According

[21] "Tanker's impossible voyage signals new sanction evasion ploy," *The Spokesman-Review*, May 28, 2021. (https://www.spokesman.com/stories/2021/may/28/tankers-impossible-voyage-signals-new-sanction-eva)
[22] Rebecca M. Nelson, James K. Jackson, and Martin A. Weiss, "The U.S. Dollar as the World's Reserve Currency," *Congressional Research Service*, December 18, 2020, page 1. (https://crsreports.congress.gov/product/pdf/IF/IF11707)
[23] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 3. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)

to a 2021 report by the UN Panel of Experts on North Korea, Pyongyang also relies on corporate service providers in third countries to facilitate its sanctions evasion activities.[24]

One example of a typical North Korean sanctions-evasion practice is the export of coal to China-based companies,[25] which then send small payments to front, shell, or trading companies in Asia or in offshore jurisdictions. These companies will then sell the coal to other markets and use the proceeds to purchase goods on behalf of North Korea. In addition to selling coal, North Korean front companies often use companies in the shipping, import/export, textile, garment, fishery, and seafood sectors to conduct their business.

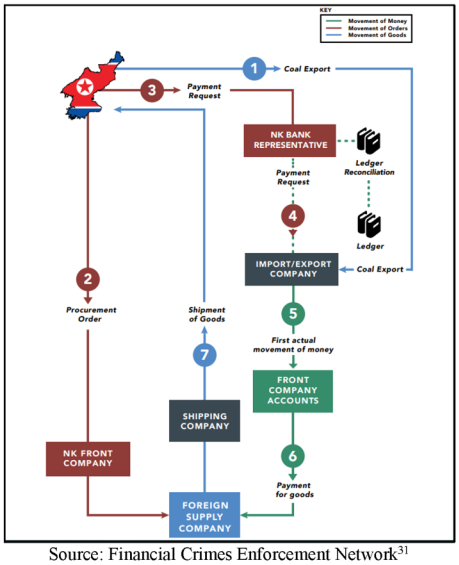
To obscure these front companies' ties to North Korea, North Korean diplomatic personnel and other overseas representatives establish bank accounts in foreign countries and set up front companies in jurisdictions with lax corporate registration practices. These companies will frequently share the same business registration address as other front companies, and different front companies with a shared address may make several payments to the same beneficiary.[26]

A recently unsealed 2018 DOJ indictment against a North Korean individual and his network of front companies for circumventing North Korea sanctions provides a case in point.[27] The indictment highlights the steps taken by the network to conceal its ties to North Korea, including the use of front companies by North Korean banks to process payments; using third-party companies to make payments; using bank accounts not in their own name; removing references to North Korea from wire transactions and transaction documents; and listing false end destinations on shipping documents that did not reference North Korea.[28]

Other countries help North Korea evade U.S. and UN sanctions as well, notably Russia and China. Between 2017 and 2018, a Russian financial services company, Russian Financial Society, helped North Korea access the international financial system by opening bank accounts for a North Korean company owned or controlled by the U.S.- and UN-designated Foreign Trade Bank (FTB).[29] As a result, North Korea gained access to the global financial system to generate revenue for its nuclear program. China similarly appears to assist – or at least tacitly condone – North Korean efforts to access the broader financial system. For instance, the 2021 UN Panel of Experts

[24] UN Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," S/2021/211, March 4, 2021, page 418. (https://undocs.org/S/2021/211)
[25] Michael R. Gordon, "Covert Chinese Trade With North Korea Moves Into the Open," *The Wall Street Journal*, December 7, 2020. (https://www.wsj.com/articles/covert-chinese-trade-with-north-korea-moves-into-the-open-11607345372)
[26] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 7. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[27] U.S. Department of Justice, Press Release, "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," March 22, 2021. (https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses)
[28] Indictment, *United States of America v. Mun Chol Myong*, 1:19-cr-00147-RC (D.D.C. filed March 22, 2021), page 9. (https://www.justice.gov/opa/press-release/file/1379211/download)
[29] U.S. Department of the Treasury, Press Releases, "Treasury Designates Russian Financial Institution Supporting North Korean Sanctions Evasion," June 19, 2019. (https://home.treasury.gov/news/press-releases/sm712).

report notes that FTB appears to continue to operate China-based accounts despite Beijing's claims to the contrary.[30]



Source: Financial Crimes Enforcement Network[31]

Iran

Central Bank of Iran Officials

Iran's regime has used a global network of front, shell, and trading companies[32] to gain access to the financial system to generate revenue and move money to support its malign activities, including human rights abuses, support for terrorist groups, and ballistic missile development. Notably, Iran has used senior officials of the Central Bank of Iran (CBI) and regional financial institutions to acquire hard currency and to conduct transactions in support of the Islamic Revolutionary Guards

[30] United Nations Security Council, "Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)," March 4, 2021, (https://undocs.org/S/2021/211), p. 52.
[31] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on North Korea's Use of the International Financial System," November 2, 2017, page 4. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[32] Trading companies are entities that are not licensed to transmit funds but that in practice operate as exchange houses and rely upon their bank accounts to transmit funds on behalf of third parties. See: U.S. Department of the Treasury, Office of Foreign Assets Control, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," *Iranian Transactions and Sanctions Regulations*, January 10, 2013, page 1. (https://home.treasury.gov/system/files/126/20130110_iran_advisory_exchange_house.pdf)

Corps Qods Force (IRGC-QF), as demonstrated by the U.S. Treasury Department's May 2018 designation of the CBI governor.[33]

The IRGC-QF is also known to use front companies to retrieve funds from foreign bank accounts held by the CBI. In one documented case, the IRGC-QF used a front company it controlled to receive millions of dollars in transfers from the CBI.[34]

Currency Exchange Houses

Iran also uses currency exchange houses[35] in third countries and trading companies to hide the origin of funds and to procure U.S. dollars. For instance, in May 2018, the United States and the United Arab Emirates disrupted a currency exchange network operating in the United Arab Emirates that procured and transferred millions in dollar-denominated bulk cash to the IRGC-QF. To do so, this network established three front companies and forged documents to mask their true purpose of funding the Iranian regime.[36] Front companies and individuals and entities involved in this type of scheme will also seek to mask Iranian involvement by omitting Iranian addresses and names of companies and individuals from key documents and will use multiple exchange houses to avoid scrutiny.

Source: Financial Crimes Enforcement Network[37]

[33] U.S. Department of the Treasury, Press Release, "Treasury Targets Iran's Central Bank Governor and an Iraqi Bank Moving Millions of Dollars for IRGC-Qods Force," May 15, 2018. (https://home.treasury.gov/news/press-releases/sm0385)

[34] U.S. Department of the Treasury, Press Release, "Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran," March 26, 2020. (https://home.treasury.gov/news/press-releases/sm957)

[35] Third-country exchange houses are financial institutions licensed to conduct foreign exchange and transmit funds on behalf of individuals and companies.
U.S. Department of the Treasury, Office of Foreign Assets Control, "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran," *Iranian Transactions and Sanctions Regulations*, January 10, 2013, page 1.
(https://home.treasury.gov/system/files/126/20130110_iran_advisory_exchange_house.pdf)

[36] U.S. Department of the Treasury, Press Release, "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF," May 10, 2018.
(https://home.treasury.gov/news/press-releases/sm0383)

[37] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018, page 3.
(https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf)

Procuring Sensitive Goods

Iran also uses front and trading companies to skirt sanctions that would otherwise prevent it from acquiring sensitive goods or services, including dual-use equipment to aid its ballistic missile development goals and commercial aviation equipment to maintain its aviation industry. Iran has also used trading companies to gain access to critical U.S. and foreign-made inputs needed to further its missile development program.

One prominent example of Iran's use of these companies was revealed by Treasury's February 2017 action targeting a series of networks that used trading companies and intermediaries to procure dual-use and other goods for the regime in Iran. To obscure the true nature of these fund transfers, members of one targeted network used a group of China-based brokers and companies to assist in the procurement of dual-use goods for the ultimate benefit of the Iranian regime. In this scheme, the China-based brokers and companies would purchase dual-use goods from other suppliers based in China and arrange shipment of those goods to Iran in exchange for financial compensation.[38]

c. The Use of Cryptocurrency

Terrorist organizations and rogue regimes have likewise used different types of cryptocurrency to evade U.S. sanctions and finance their activities. While cryptocurrencies – and the blockchain on which they are often based – can provide a significant degree of transparency and the ability to trace and seize illicit funds transfers,[39] certain cryptocurrencies provide a degree of anonymity that can be exploited by terrorist organizations and rogue regimes. In recent months, we have seen a range of ways in which malign actors have exploited cryptocurrencies to evade sanctions.

Terrorist organizations have aggressively used cryptocurrencies to receive donations and evade sanctions. For example, in 2020, DOJ disrupted three separate campaigns by the al-Qassam Brigades, Hamas' military wing; al-Qaeda; and Islamic State. According to DOJ,

> In the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps. The al-Qassam Brigades boasted that bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor.[40]

---

[38] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Supporters of Iran's Ballistic Missile Program and Iran's Islamic Revolutionary Guard Corps – Qods Force," February 3, 2017. (https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx)

[39] David Uberti, "How the FBI Got Colonial Pipeline's Ransom Money Back," *The Wall Street Journal*, June 11, 2021. (https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981)

[40] U.S. Department of Justice, Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," August 13, 2020. (https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns)

Likewise, according to DOJ, al-Qaeda "operated a bitcoin money laundering network using Telegram channels and other social media platforms to solicit cryptocurrency donations to further their terrorist goals. In some instances, they purported to act as charities when, in fact, they were openly and explicitly soliciting funds for violent terrorist attacks."[41]

During and after the conflict between Israel and Hamas in late spring 2021, Hamas apparently received a significant uptick in donations in the form of bitcoin. According to a senior Hamas official, the group saw "a surge in cryptocurrency donations since the start of the armed conflict with Israel" last month, "exploiting a trend in online fundraising that has enabled it to circumvent international sanctions to fund its military operations."[42]

Likewise, Iran may be using bitcoin mining to circumvent sanctions. Despite the primary and secondary sanctions that prohibit or make sanctionable almost all activity in the Iranian energy sector, Iran has turned to bitcoin mining as one way to mitigate the impact of the restrictions on its oil sector. According to the cryptocurrency diligence firm Elliptic, up to 4.5 percent of worldwide bitcoin mining may take place in Iran.[43] While Iran cannot easily export its energy products because of the sanctions maintained by the United States, persons in Iran can use Iranian energy products to mine bitcoin, which is an energy-intensive process.[44]

Mining bitcoin provides a way for Iranians to earn revenue, and it is estimated that the amount of bitcoin mined in Iran could equal approximately $1 billion annually.[45] Iranian think tanks have recognized the potential for sanctions evasion, noting that bitcoin may not be traceable and can be used on international exchanges.[46] This extensive bitcoin mining raises clear compliance questions, including how bitcoin mined in Iran and inserted into international cryptocurrency markets can be identified or potentially overlooked by entities operating in these markets. Recent press reporting also suggests that Iran has cracked down on bitcoin mining in the country, in part because the extensive energy needs of mining have led to blackouts across the country.[47]

In addition, state actors such as North Korea have engaged in hacking operations of virtual currency exchanges to steal cryptocurrency. For example, in March 2020, DOJ charged two Chinese nationals with laundering over $100 million worth of cryptocurrency from a hacked

---

[41] Ibid.
[42] Benoit Faucon, Ian Talley, and Summer Said, "Israel-Gaza Conflict Spurs Bitcoin Donations to Hamas," *The Wall Street Journal*, June 2, 2020. (https://www.wsj.com/articles/israel-gaza-conflict-spurs-bitcoin-donations-to-hamas-11622633400)
[43] Tom Robinson, "How Iran Uses Bitcoin Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil," *Elliptic*, May 21, 2021. (https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions)
[44] Ibid. China has reportedly established significant bitcoin mining farms in Iran.
[45] Ibid.
[46] Behnam Gholipour, "Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions," *IranWire*, March 2, 2021. (https://iranwire.com/en/features/9084)
[47] Shivam Vahia, "Iran is planning to introduce a legal framework for crypto even as Bitcoin mining activity remains restricted," Business Insider, June 10, 2021. (https://www.businessinsider.in/cryptocurrency/news/iran-is-planning-to-introduce-a-legal-framework-for-crypto-even-as-bitcoin-mining-activity-remains-restricted/articleshow/83396588.cms)

cryptocurrency exchange for the ultimate benefit of the North Korean regime.[48] The funds were then laundered through hundreds of automated cryptocurrency transactions aimed at preventing law enforcement from tracing the funds. The individuals circumvented compliance controls by submitting doctored photographs and falsified identification documentation, utilizing over 100 virtual currency accounts and addresses, and transferring over $1 million into prepaid iTunes gift cards.

One emerging area of concern in the cryptocurrency and blockchain space relates to decentralized financial products and services, known as DeFi. DeFi is a blockchain-based set of products and services that facilitates transactions directly between parties without the use of a centralized financial intermediary.

In many cryptocurrency transactions, the transaction will be intermediated by an exchange. In such a situation, the exchange likely has compliance obligations, including to ensure that the transacting parties are not sanctioned persons. Decentralized financial products do not rely on such an intermediary. Instead, individuals can buy and sell financial products directly with one another through smart contracts. Usually created by software developers, such smart contracts can trigger transactions when certain conditions obtain – for example, when the price for a certain cryptocurrency reaches a particular threshold. They generally allow people to lend or borrow funds from others, trade cryptocurrencies, and engage in a wide range of additional financial transactions.

Such decentralized products and services pose significant sanctions-compliance challenges. For example, determining whether a party to a particular one-to-one transaction is a sanctioned person may be complex, though this challenge could be mitigated depending on the transparency requirements specified in the smart contract or in the community governing its terms. Likewise, DeFi may pose risks that sanctioned parties are able to transact and receive items of value without their counterparties knowing that they are sanctioned or even being aware that they may be prohibited from transacting with such persons. (For example, an individual conducting a transaction may not understand that he or she cannot transact with a sanctioned person.) As a result, there may be significant risks that sanctioned parties can use these products and services to evade sanctions.

The nature of decentralized finance poses particular challenges to the effectiveness of U.S. sanctions programs and the Treasury Department's ability to extend its reach far beyond its resources. Treasury has a long history of focusing its regulations and enforcement actions on key gatekeepers in certain industries. For example, by ensuring that financial institutions understand and take their sanctions-compliance obligations seriously, Treasury can leverage its resources more effectively to root out illicit actors in the financial system. Likewise, in the case of the shipping industry, the Treasury and State departments focus on deputizing companies in this sector to target international trade prohibited under U.S. sanctions. Treasury and State do not have the resources to effectively regulate global financial transactions and commerce, but by ensuring that

[48] U.S. Department of Justice, Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack," March 2, 2020. (https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack)

key gatekeepers must comply with U.S. sanctions laws and regulations, they can have a far-outsized impact.

With centralized cryptocurrency exchanges, Treasury will likely continue to focus on their role as a key gatekeeper in this ecosystem and push to ensure they have effective sanctions-compliance programs in place (through a combination of guidance and enforcement activity). However, with DeFi, no clear gatekeeper exists. Indeed, in many ways, that is the impetus behind the creation and rise of DeFi products. This means that Treasury may need to find new and innovative ways to ensure that sanctioned parties do not attempt to widely exploit DeFi.

VI. Effectively Blunting Sanctions Evasion Requires a Defense-in-Depth Approach

The U.S. government, its allies and partners, and the private sector must adopt a multilayered, "defense-in-depth" approach to effectively counter sanctions evasion. Each layer of defense decreases the chances that a terrorist organization or rogue regime can access to global markets. And while each layer may not be foolproof, together they can pose a formidable obstacle. Elements of this defense-in-depth approach include:

- *Effective Intelligence Collection.* Key to effectively countering sanctions evasion activity is the ability to detect such activity in the first instance. The Treasury Department's Office of Intelligence and Analysis (OIA), along with other members of the intelligence community, as well as FinCEN, should be provided the tools necessary to identify sanctions evasion. A legislative proposal under consideration by this committee, the OFAC Fusion Center Act, could help achieve this. The law would create an interagency group designed to share data and allow for better detection and disruption of illicit networks, including sanctions evaders. While an OFAC Fusion Center may have broader responsibilities and authorities, the intelligence-collection component should be a major element. Note that Treasury has previously worked on related initiatives in sanctions program-specific contexts.

- *Aggressive Designation Activity.* OFAC should continue to aggressively target sanctions evaders. In particular, OFAC should focus on targeting financial facilitators of evasion activity as well as entire evasion networks. For example, in the North Korea context, OFAC has sanctioned over 40 North Korean, Russian, Chinese, Singaporean, Burmese, and Thai financial facilitators who have helped the North Korean regime launder funds. The facilitator plays one of the most valuable roles for the North Korean regime: providing access to the global economy. The North Korean regime has a hard time finding third-country nationals they can trust to handle all its illicit needs. Exposing and sanctioning these individuals cuts the regime's access and obstructs the flow of funds.

In addition, targeting entire networks can be an effective approach for disrupting evasion activity.[49] For example, last year OFAC acted against an Iranian-Venezuelan network by designating the network's shipping companies, vessels, and vessel captains for delivering gasoline to Venezuela.[50] Although it may have appeared to be a routine designation, this was a landmark action, as OFAC had not previously targeted vessel captains. This action signaled to the maritime community that OFAC will hold all parties responsible and is willing to act against entire networks that facilitate sanctions evasion, not just the shipping companies themselves. This increased the incentives for compliance across the industry. The more that OFAC can designate entire networks, the less likely persons in those networks will be to engage in sanctions evasion in the future.

- *Providing the Private Sector With the Right Tools*. A critical element in the fight against sanctions evasion is ensuring that the private sector has the right tools to identify and disrupt such activity. As discussed, Treasury does not have the resources to monitor the full scope of global financial and trade transactions. In recent years, Treasury and the U.S. government more broadly have tried to arm the private sector with information on sanction-evasion tactics and red flags that can help companies spot sanctions evasion. Combined with clearly signaling to the private sector their compliance obligations and pursuing aggressive enforcement actions against those who fail to comply, this additional information can help the private sector more effectively counter evasion activity.

  In recent years, Treasury, State, and other agencies have provided the private sector with a substantial amount of information in the form of a range of advisories focused on Iranian,[51] North Korean,[52] Venezuelan,[53] and Syrian[54] sanctions-evasion tactics, as well as broader advisories focused on sanctions evasion in particular sectors.[55] This

[49] Under Secretary of the Treasury for Terrorism and Financial Intelligence, *Speech Delivered at the Center for Strategic and International Studies*, July 31, 2019. (https://home.treasury.gov/news/press-releases/sm748)
[50] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Five Iranian Captains Who Delivered Gasoline to the Maduro Regime in Venezuela," June 24, 2020. (https://home.treasury.gov/news/press-releases/sm1043)
[51] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018. (https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf)
[52] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "FinCEN Advisory on North Korea's Use of the International Financial System," November 2, 2017. (https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf)
[53] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "Updated Advisory on Widespread Public Corruption in Venezuela," May 3, 2019. (https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf)
[54] U.S. Department of the Treasury, Financial Crimes Enforcement Network, Advisory, "OFAC Advisory to the Maritime Petroleum Shipping Community," November 20, 2018. (https://home.treasury.gov/system/files/126/syria_shipping_advisory_11202018.pdf)
[55] See, for example: U.S. Department of the Treasury, U.S. Department of State, and U.S. Coast Guard, Advisory, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," May 14, 2020. (https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf)

administration should continue and expand on this approach. To that end, the potential creation of an OFAC Exchange designed to help provide the private sector with information on illicit activity, red flags, and trends[56] could be an effective way to supplement the information provided to the private sector on sanctions evasion methods and typologies.

- *Identifying and Tackling Emerging Areas of Risk*. Critical to ensuring that our adversaries are not able to exploit new technologies and products is identifying and addressing the sanctions risks those technologies and products may pose. For some time, Treasury has been focused on the risks (and opportunities) presented by cryptocurrencies and digital assets more broadly. However, as certain products and services that present significant sanctions risks are more widely adopted, Treasury should clearly communicate its compliance expectations to the broader cryptocurrency community. Likewise, to the extent possible, it should identify relevant gatekeepers within the community to try to enlist as partners in combating sanctions-evasion activity.

- *Internationalizing the Fight*. Financial integrity – and the ability to effectively detect, disrupt, and deter sanctions evasion – is often only as strong as its weakest link. For example, if sanctions evaders and other illicit actors can set up front and shell companies in other jurisdictions and use those companies to access the U.S. financial system or other important financial systems, our efforts at countering sanctions evasion will be significantly hampered. While the United States has done a good job in recent years of pushing the financial integrity mission in conjunction with its allies and partners and in multilateral fora such as the Financial Action Task Force, our efforts to promote sanctions compliance abroad through the development and implementation of key standards and jurisdictional authorities to address these issues remain incomplete.

VII. Conclusion

To ensure that our sanctions programs remain effective and help us achieve national security objectives, Congress, the administration, and the private sector must all work together to help identify, disrupt, and deter sanctions evasion. While this is a challenging task, an approach that emphasizes aggressive designations, clear communication to the private sector regarding compliance obligations and red flags, and efforts to ensure regulations and guidance effectively address risks with new and innovative products and services will best position the United States to continue to have effective and powerful sanctions tools.

I look forward to your questions and thank you again for the opportunity to testify.

---

[56] Note that the OFAC Exchange could mirror the approach taken by the FinCEN exchange. U.S. Department of the Treasury, Financial Crimes Enforcement Network, Press Release, "FinCEN Launches 'FinCEN Exchange' to Enhance Public-Private Information Sharing," December 4, 2017. (https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing)

Chainalysis

Written Testimony of Jesse Spiro
Chief of Government Affairs
Chainalysis

Before the
House Financial Services Committee
Subcommittee on National Security, International Development and Monetary Policy

Hearing on
Schemes and Subversion:
How Targets of Sanctions Undermine and Evade Sanctions Regimes

Wednesday, June 16, 2021

Chairman Himes, Ranking Member Barr, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this very important topic.

My name is Jesse Spiro and I am the Chief of Government Affairs at Chainalysis. Chainalysis is the blockchain analysis company. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely. I am very glad to be here today to speak about sanctions. Every year, Chainalysis publishes a widely-read annual Crypto Crime Report, and sanctions are one of the items we focus on in the report.

Chainalysis' mission is to build trust in blockchains, and we provide blockchain data and analysis that enables law enforcement to investigate illicit activities, and regulators to ensure compliance with anti-money laundering and sanctions requirements. We also serve customers in the cryptocurrency and financial sectors, enabling them to remain in compliance with all of the latest regulatory developments, including guidance from the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). As this rather new ecosystem grows, it is important that people have confidence in it.

Today I would like to discuss:

1. How blockchain data and analysis can benefit investigations into sanctions evasion using cryptocurrency,
2. Sanctions and cryptocurrency,
3. Examples of illicit actors and adversarial groups that have have employed cryptocurrency to evade sanctions,
4. Challenges and successes under the current sanctions regime, and
5. Recommendations for ways to improve the current sanctions regime with regards to cryptocurrency.

I would like to note that while the focus of today's hearing is sanctions, and cryptocurrency is one way that illicit actors evade sanctions, the vast majority of cryptocurrency transactions are legitimate. According to our analysis, in 2020, the illicit share of all cryptocurrency activity was just 0.34%, or $10.0 billion in transaction volume. This was a decrease from 2019, when illicit activity represented 2.1% of all cryptocurrency transaction volume, or roughly $21.4 billion worth of transfers. We do expect 2020's reported illicit activity numbers to rise slightly over time as we learn more about scams, fraud, and other illicit activity that have not yet been identified, but it is clear the vast majority of transactions are legitimate in nature.

How Blockchain Data and Analysis Can Benefit Investigations into Sanctions Evasion Using Cryptocurrency

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone can look up the entire history of transactions on these blockchains. The ledger shows a string of random numbers and letters that transact with another string of random numbers and letters. At its core, Chainalysis is a data company, and our data set maps these random numbers and letters – cryptocurrency addresses– to their real-world entities. For example, in Chainalysis products, we are able to see that a given transaction was between a user at a specific exchange, with a user at another exchange, or between a user at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency.

Our data set and investigative tools are invaluable in allowing investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency. Using blockchain analysis tools, law enforcement can trace cryptocurrency to identify its origination and/or its cashout points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money service businesses here in the United States and collect Know Your Customer (KYC) information from their customers. In their response to legal process, the exchange will provide any identifying information that they have related to the cryptocurrency address, such as name, address, and government identification documentation, to law enforcement, allowing them to further their investigation.

In part due to the ability to leverage the transparency of cryptocurrencies and blockchain analytics, law enforcement has been able to disrupt terrorist financing campaigns, dismantle child sexual abuse material websites, and seize the ill-gotten proceeds of Darknet marketplace administrators.

Blockchain analysis tools like ours are also used by financial institutions and cryptocurrency exchanges to ensure they are meeting their anti-money laundering requirements. These tools can detect and alert users to patterns of potential high-risk activity among their

customers. Using these tools, businesses can identify whether their customers are attempting to transact with OFAC sanctioned individuals, entities, or jurisdictions, or cashing out funds generated from Darknet markets, scams, fraud, and other forms of illicit activity.

Blockchain and investigative analyses can be used to determine ownership or control of additional addresses associated with sanctioned individuals or entities based on information OFAC has provided publically. For example, if OFAC lists a cryptocurrency address as an identifier associated with a particular individual, using blockchain analytics, we can identify other wallet addresses likely controlled by the same individual and label them so that they are also identified as belonging to the sanctioned individual. Likewise, additional assets, such as tokens or forks of blockchains, associated with the addresses and entities identified by OFAC can be determined through blockchain analytics.

When OFAC lists cryptocurrency addresses as identifiers associated with sanctioned entities, they are labelled in our tools as sanctions-related and our customers receive alerts on historical or future exposure to these addresses. This means our technology enables cryptocurrency exchanges and financial institutions to ensure that their customers are not interacting with addresses associated with sanctioned persons and identify and freeze any accounts that attempt to do so.

Blockchain analytics can also be used to identify trends and develop intelligence about who may be facilitating the evasion of sanctions. Using tools like the ones that Chainalysis develops, it's possible to quantify how much sanctions evasion has occurred in the past, something that would not be possible in traditional finance. For example, by tracking their payments, our customers can identify virtual private network (VPN) services, bulletproof web hosting services, and other providers sanctioned malicious actors are using. All of this information is valuable intelligence that can allow investigators to determine new trends and patterns in sanctions evasion so that they can combat them.

Because of its inherent transparency and traceability, there are many advantages to cryptocurrency when it comes to investigating sanctions evasion. Traditionally, criminals and money launderers have attempted to use misspellings, code words, and other techniques to evade sophisticated sanctions screening. But with cryptocurrency, the unforgeable addresses represent unavoidable, definitive evidence on a transparent record. Additionally, unlike some forensic evidence that degrades over time, blockchain evidence is permanent and immutable. What's more, our ability to analyze this evidence is only getting more sophisticated. Criminals who thought they evaded detection in months and years past often find they've left a permanent trail for law enforcement to follow.

Sanctions and Cryptocurrency

OFAC is charged with administering and enforcing economic and trade sanctions. This includes sanctions against terrorists, transnational criminal organizations, those engaged in activities related to the proliferation of weapons of mass destruction, and foreign countries that pose a threat to our national security. OFAC creates and maintains the Specially

Designated Nationals and Blocked Persons List (SDN List), which financial institutions screen their customers against. In addition to the SDN List, there are comprehensive country and regional embargoes. U.S. persons are prohibited from engaging in a wide range of activity in connection with individuals or entities on OFAC's SDN List and those covered by comprehensive country or region embargoes.

In 2015, then-President Obama issued Executive Order 13694, titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," and OFAC began designating malicious cyber actors. Since then, OFAC has implemented a cyber sanctions program and designated many malicious cyber actors, including perpetrators of ransomware attacks, actors who have stolen millions in cryptocurrency from users in exchange hacks, and those who facilitate ransomware or theft proceeds by exchanging them for fiat.

In March 2018, OFAC released public guidance [FAQs #559, 560-594] related to cryptocurrencies and indicated they would start listing "digital currency addresses" on the SDN List as identifiers associated with sanctioned individuals and entities. In November 2018, OFAC designated two Iran-based financial facilitators of malicious cyber activity for their alleged involvement in the SamSam ransomware, and for the first time included digital currency addresses as identifiers.

On the SDN list, OFAC lists cryptocurrency addresses under sanctioned entities or individuals as identifier "Digital Currency Address" as shown in the example below.

Example of OFAC "Digital Currency Address" Listing

Details:

Type:	Individual	**List:**	SDN
Last Name:	KHORASHADIZADEH	**Program:**	CYBER2
First Name:	Ali	**Nationality:**	Iran
Title:		**Citizenship:**	
Date of Birth:	21 Sep 1979	**Remarks:**	
Place of Birth:	Tehran, Iran		

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Passport	T14553558	Iran	28 Oct 2008	29 Oct 2013
Digital Currency Address - XBT	149w62rY42aZBox8fGcmqNsXUzSStKeq8C			
Gender	Male			
Email Address	iranvisacart@yahoo.com			
Email Address	alikhorashadi@yahoo.com			
Email Address	mastercartaria@yahoo.com			
Email Address	toppglasses@gmail.com			
Email Address	iranian_boy5@yahoo.com			
Additional Sanctions Information -	Subject to Secondary Sanctions			

Aliases:

Type	Category	Name
a.k.a.	weak	Mastercartaria
a.k.a.	weak	Iranvisacart

Since November 2018, OFAC has included 97 digital currency addresses in eight different designations. This has included designations against Chinese nationals for narcotics trafficking and money laundering, associates of the Democratic People's Republic of Korea (DPRK) Lazarus Group, Russian nationals for their involvement in disinformation campaigns, and Russian cyber actors involved in cryptocurrency exchange hacks. In April of this year, the Biden Administration announced several new sanctions against Russian intelligence service disinformation outlets and designated a Pakistani organization that provided cyber actors, including Russian disinformation actors, fraudulent identity documents used in the digital onboarding process at financial institutions.

In October 2020, OFAC issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments." The advisory warned, "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, not only encourage future ransomware payment demands but also may risk violating OFAC regulations." OFAC's alert bolstered previous government guidance not to pay ransomware attackers, who typically demand ransom be paid in cryptocurrency, as this incentivizes future attacks and goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations. It also noted that license applications made to OFAC that involve ransomware payments demanded as a result of malicious cyber-enabled activities would be reviewed by OFAC, but with a presumption of denial.

Under 2013 guidance from FinCEN, cryptocurrency exchanges must register as money services businesses ("MSBs"). They therefore must meet certain anti-money laundering/countering the financing of terrorism (AML/CFT) requirements under the Bank Secrecy Act, including (i) establishing AML programs, (ii) adhering to certain regulatory reporting requirements, and (iii) maintaining certain books and records. This includes complying with sanctions regulations. This has led US-based cryptocurrency exchanges to establish KYC programs to verify the identity of their customers and use transaction monitoring solutions to detect suspicious activity, making it more difficult for illicit actors or those trying to evade sanctions to cash out their ill-gotten cryptocurrency for fiat currency.

More recently, after a number of high-profile ransomware attacks, including those on Colonial Pipeline and JBS, National Security Advisor Jake Sullivan confirmed the Administration would be addressing the issue of ransomware and "countries, including Russia, that are harboring or permitting cyber criminals to operate from their territory" at the G7 Summit. While the addition of cryptocurrency addresses as identifiers for sanctioned individuals and entities is a relatively new advent, we see based on blockchain data how impactful these inclusions are. The data on ransomware specifically suggests that blockchain analysis will be crucial to fighting cybercrime from groups aligned with Russia and other hostile nation states.

Examples of Illicit Actors and Adversarial Groups That Have Employed Cryptocurrency to Evade Sanctions

Terrorist Groups

While terrorist financing using cryptocurrency is a small portion of the illicit activity we see on the blockchain, it does occur. Cryptocurrency as a terrorism financing tool presents particular challenges. Unlike social media profiles and bank accounts, a cryptocurrency address is much more difficult to shut down due to the decentralized nature of blockchains. Here I outline several examples of terrorist organizations that have exploited cryptocurrency as a means of evading sanctions and raising money for their violent efforts.

Terrorist Groups: Hamas

Recently, a representative from Palestinian militant group Hamas confirmed that they have seen an increase in cryptocurrency donations. The group is able to use cryptocurrency to circumvent international sanctions to fund its military operations. This is not a new trend for the group, which has exploited cryptocurrency in the past to raise money.

The Izz ad-Din al-Qassam Brigades (AQB) is the military wing of Hamas, a U.S.- and European Union-designated terrorist organization. Chainalysis has written previously about AQB's use of cryptocurrency in donation campaigns in our 2020 Crypto Crime Report and in August 2020, the U.S. federal authorities seized more than $1 million in cryptocurrency tied to AQB financial facilitators.

AQB's campaign started in 2019, when they posted a call on their social media page and official websites asking for Bitcoin donations. According to the DOJ's press release, "The al-Qassam Brigades boasted that Bitcoin donations were untraceable and would be used for violent causes. Their websites offered video instruction on how to anonymously make donations, in part by using unique Bitcoin addresses generated for each individual donor." Federal investigators were able to employ blockchain analysis to track the donated cryptocurrency and take action by identifying individuals who had violated U.S. sanctions by donating to the terrorists or individuals who received Bitcoin from the campaign.

Terrorist Groups: Al-Qaeda

Al-Qaeda, another U.S.- and European Union-designated terrorist organization, along with affiliated groups, operated a cryptocurrency terror finance campaign, evading U.S. sanctions. The campaign was conducted using Telegram and other social media platforms to solicit donations to fund violent terrorist attacks and equip terrorists in Syria. U.S. law enforcement was able to identify 155 virtual currency addresses associated with the terrorist campaign.

According to the criminal complaint, these al-Qaeda and affiliated groups used multi-layered transactions to obfuscate the movement of these donations to a central hub of

addresses, from which funds were then redistributed to the individual groups. Through blockchain analysis, Chainalysis identified the BitcoinTransfer Office in Idlib, Syria as the central hub described in the criminal complaint. BitcoinTransfer purports to be a cryptocurrency exchange but has been implicated in several terrorism financing schemes and appears to be fully under the control of terrorist groups. Since the service became active in late December 2018, more than $280,000 worth of Bitcoin has passed through BitcoinTransfer, much of it related to terrorism financing.

While multiple terrorist groups ran their own individual donation pushes, nearly all of them followed a similar strategy. The groups presented themselves as charitable organizations operating in Syria to solicit Bitcoin donations on social media and messaging platforms — mostly Telegram and Facebook. However, despite the charity facade, these groups often published posts indicating that donations would go towards purchasing weapons for militant groups.

In May 2019, U.S. law enforcement monitoring the Telegram page of one such group, Tawheed & Jihad Media, saw the administrators promoting a funding campaign for "bullets and rockets for the *mujahideen*" with a single Bitcoin address listed. Law enforcement monitored that address as donations came in, and noticed that the group administrators eventually moved the funds to an address associated with BitcoinTransfer.

Using similar analytical techniques, law enforcement observed terrorism financing campaigns conducted by other al-Qaeda-affiliated groups, most of whom solicited donations in similar ways — pretending to be charities while actually funding militant activity — before sending the proceeds on to al-Qaeda's BitcoinTransfer addresses. Those groups include:

- Malhama Tactical - a jihadist military company that trains Hay'at Tahrir al-Sham (HTS) fighters and has solicited Bitcoin to finance HTS operations in Syria.
- Al Sadaqah - "charity" in Arabic, is a Syrian organization that operates social media accounts on multiple platforms which seek to finance terrorism via Bitcoin solicitations.
- Al Ikhwa - the group's profile describes them as an "independent charity on the ground in Syria" and that they "do not support any acts of terrorism;" however, blockchain analysis and a review of related social media posting demonstrates otherwise.
- Reminder from Syria - a Telegram channel affiliated with terrorist groups that frequently interacts with and boosts content from Al Ikhwa on social media.

Given these instances, it's crucial that cryptocurrency businesses and financial institutions monitor transactions to address any possible exposure to terrorist financing campaigns.

Nation States

At both the government-level and the individual-level those in nation states impacted by sanctions have embraced cryptocurrency adoption for various reasons. For some it is simply

out of curiosity or investment, for others it is about wealth preservation to hide from their government's reach, and then there are those who are using it as a way to evade sanctions, or facilitate financial cyber crimes. Below I outline examples from Iran, Russia, North Korea, and Venezuela.

Nation State Actors: Iran

Iranian officials have discussed the use of cryptocurrencies to evade sanctions, with Iranian researchers preparing whitepapers on the topic. The Central Bank of Iran has piloted research and development of a Central Bank Digital Currency (CBDC). Recently, Iranian President Hassan Rouhani requested his government start developing a framework to regulate cryptocurrencies. Beyond the government level, Iran's citizens have embraced cryptocurrency and are considered early adopters. The two main ways Iran can use cryptocurrency to evade sanctions, or weaken the impact of sanctions, is to acquire wealth by mining or theft of cryptocurrencies, or to use cryptocurrencies to conduct economic business to bypass traditional screening.

Iran is heavily involved in mining cryptocurrencies. By mining cryptocurrencies, Iran is able to acquire wealth by validating cryptocurrency payments for individuals globally - including U.S. citizens. They can then transact via non-traditional financial institutions, including high risk exchanges or individual peer-to-peer traders, to bypass screening. Iran's cyber actors have been involved with deploying ransomware and receiving cryptocurrency payments from U.S. companies.

While there has not been substantial reporting on exact use cases for economic trades involving cryptocurrency, Iran could use cryptocurrency to send and receive payments for oil or other goods to evade sanctions. According to a report from the English-language Iranian economic news source Financial Tribune, the Central Bank of Iran is authorizing banks and licensed exchanges to use cryptocurrency as payments for imports.

Chainalysis research has identified over 20 Iranian exchanges that have received cryptocurrencies worth over $820 million since May 2013. Substantial amounts of the Bitcoin received at these exchanges can be traced back to mining operations or exchanges not based in Iran, while substantial amounts of the outgoing Bitcoin can be traced to various exchanges located around the world.

Nation State Actors: Russia

Russian cybercriminals are involved in developing and deploying ransomware, cryptocurrency thefts from individuals and exchanges, and cryptocurrency scams aimed to defraud cryptocurrency users. The GRU, a Russian military foreign intelligence service involved with disinformation campaigns and other cyber activities, have used cryptocurrency to acquire cyber infrastructure.

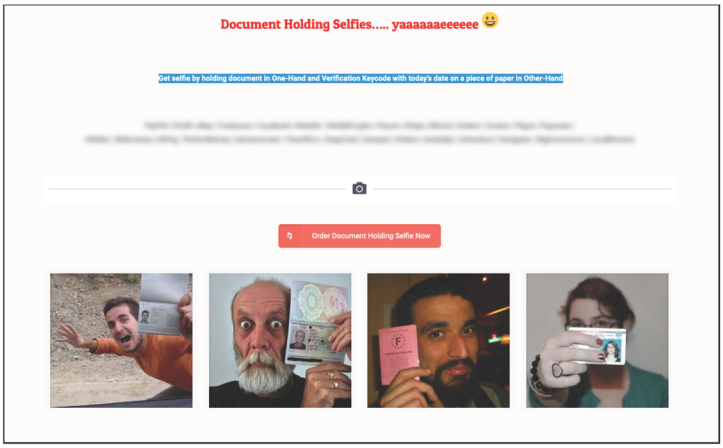
In 2020, OFAC designated Russian nationals involved with the previously designated Internet Research Agency (IRA) disinformation campaign and in a separate action they designated Russian cybercriminals involved with stealing cryptocurrencies. In April 2021, in coordination with the issuance of a new Executive Order and a six-count federal indictment from the Department of Justice, OFAC took sweeping action against 16 entities and 16 individuals who attempted to influence the 2020 U.S. presidential election at the direction of the leadership of the Russian Government. Second Eye Solution (SES), an entity designated on this date, highlights the weaknesses for digital onboarding and sanctions screening.

SES is a Pakistan-based synthetic identity document vendor that provided fake identity documents for people to sign up for accounts with cryptocurrency exchanges, payment providers, banks, and more under false identities. SES assisted the IRA in concealing its identity to evade sanctions. According to the Department of Justice indictment, SES provided documents to over 200 countries and territories. These documents can be used to bypass sanctions screening.

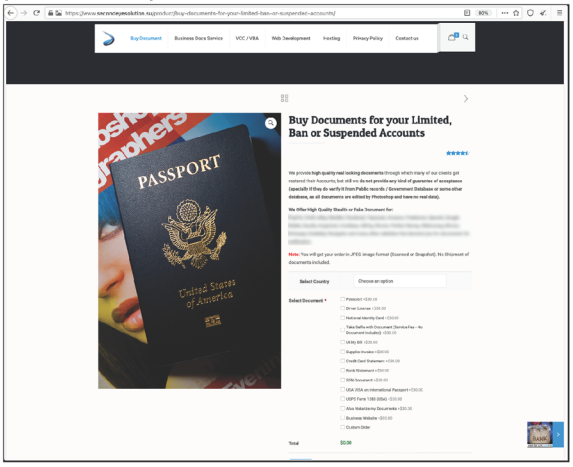
SES operated openly on the Clearnet, rather than on the Darknet like many other fraud shops and illegal businesses Chainalysis studies. The company promoted its products to people looking to sign up for financial technology (fintech) and cryptocurrency platforms using falsified documents. In fact, SES's documents were only in digital JPEG format, with no physical documents provided, making it difficult to imagine use cases other than fooling remote photo or video-based KYC checks. The company even offered users fake selfies in which they appear to be holding identifying documents — a common requirement for remote KYC checks during onboarding.

SES also helped its customers carry out synthetic identity fraud as opposed to stolen identity fraud, a rarity in fraud shops. Whereas stolen identity fraud involves the use of stolen information to steal an existing person's identity, perpetrators of synthetic identity fraud typically use a mix of real and fake information, such as social security numbers and names, to create new false identities in order to commit fraud.

Example of Second Eye Solution's Advertised Selfie Offerings



Example of Second Eye Solution's Advertised Fake Documents for Sale



After customers chose the documents they wanted to purchase, SES would ask them to specify the services at which they planned to use them so that the documents could be tailored accordingly. Most fake documents were priced between $30 and $80. Customers could pay using cryptocurrencies like Bitcoin, Ethereum, Litecoin, and Bitcoin Cash, or with online payment services like WebMoney, PerfectMoney, and Payoneer.

The DOJ indictment notes that threat actors associated with Russia's IRA bought fake identification documents from the company in order to set up online accounts under assumed identities. The IRA is a "troll farm" that uses digital and social media manipulation to push public opinion on behalf of the Russian government, and is known for having interfered in the 2016 U.S. election. OFAC previously sanctioned the IRA in March 2018, September 2019, and September 2020, and according to the Treasury, selling to the IRA is the specific offense that has now landed SES on the SDN List.

Using blockchain analytics to analyze the cryptocurrency addresses cited in OFAC's designation and those we have identified through co-spending patterns, we see that SES received over $2.5 million worth of cryptocurrency across 31,000 transactions since becoming active in 2013.

Nation State Actors: Democratic People's Republic of Korea (DPRK)

The Democratic People's Republic of Korea (DPRK) trains cyber actors to target and launder stolen funds from financial institutions. Of note is Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group. Lazarus Group is an infamous cybercriminal syndicate sponsored by the North Korean government. Considered an advanced persistent threat by cybersecurity experts, Lazarus Group is accused of being behind the 2014 hack of Sony Pictures; the 2017 WannaCry ransomware attacks, which affected at least 150 countries around the world and shut down approximately three hundred thousand computers; the $81 million Bangladesh Central Bank SWIFT hacking; as well as a number of cryptocurrency exchange attacks. Overall, the group is believed to have stolen more than $1.75 billion worth of cryptocurrency in the time it's been active. According to OFAC, "North Korea's malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges" and the stolen funds allow "the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs."

In March 2019, the DragonEx cryptocurrency exchange was hacked by Lazarus Group and lost over $7 million worth of cryptocurrency, including Bitcoin, Ripple, and Litecoin. DragonEx responded quickly, announcing on various social media platforms that it had been hacked and releasing a list of 20 wallet addresses to which its funds had been transferred. That allowed other exchanges to flag those wallets and freeze accounts associated with them, making it harder for the attackers to move the funds. Also in 2019, Lazarus hacked the UpBit cryptocurrency exchange, which netted them more than $49 million worth of cryptocurrency. Then in 2020, Lazarus Group managed to pull off the biggest cryptocurrency theft of the year, stealing roughly $275 million worth of cryptocurrency from the exchange KuCoin. According to KuCoin's CEO, the hack occurred after cybercriminals gained access to the private keys to the exchange's hot wallets. Soon after, he claimed that the exchange had recovered $204 million worth of the stolen funds.

Lazarus Group's hacking techniques have advanced over time, as evidenced in the DragonEx instance. Initially, Lazarus Group relied on social engineering to attack exchanges,

typically fooling employees into downloading malicious software that gave Lazarus access to users' funds. Lazarus took this strategy a step further and executed one of the most elaborate phishing schemes we've seen to gain access to users' funds in the 2019 DragonEx exchange hack.

While the DragonEx hack was relatively small, it was notable for the lengths Lazarus Group went to in order to infiltrate the exchange's systems in a sophisticated phishing attack. Lazarus created a fake company claiming to offer an automated cryptocurrency trading bot called Worldbit-bot, complete with a slick website and social media presence for made-up employees. Lazarus even went so far as to build a software product resembling the trading bot they claimed to be selling. The key difference, of course, was that the program contained malware giving the hackers access to the computer of anyone who downloaded it. Lazarus Group hackers pitched a free trial of the software to DragonEx employees, eventually convincing someone to download it to a computer containing the private keys for the exchange's wallets. From there, the hackers were able to make off with millions.

Similarly, Lazarus Group's money laundering techniques have advanced over time. For example, in 2018, 98% of all funds Lazarus stolen from exchanges were moved to exchanges with minimal KYC requirements. By 2019, 48% of funds stolen by Lazarus moved to mixers or CoinJoin wallets, while 50% sit unspent in the hackers' original wallet. Mixers obfuscate the path of funds by pooling cryptocurrency from multiple users, and giving each one back an amount from the pool equal to what they initially put in, minus a 1-3% service fee. Everyone ends up with a "mix" of the funds everyone else put in, which makes it more difficult to connect the inputs to an output on the users' transactions. Many criminals use mixers to hide the source of illicit cryptocurrency before moving it to other services. CoinJoin wallets (named for the underlying CoinJoin protocol), such as Wasabi Wallet, accomplish the same thing by providing a wallet service that allows multiple users to trustlessly join their payments into a single transaction with multiple recipients.

The advances Lazarus Group has made in both their hacking and money laundering techniques reveal the time and resources Lazarus has at its disposal, as well as the deep knowledge of the cryptocurrency ecosystem necessary to successfully impersonate legitimate participants and adapt to investigative techniques.

In February 2019, OFAC sanctioned Lazarus Group, as well as two of their subgroups, "Bluenoroff" and "Andariel." In the announcement of the designation, OFAC noted that, "Lazarus Group targets institutions such as government, military, financial, manufacturing, publishing, media, entertainment, and international shipping companies, as well as critical infrastructure, using tactics such as cyber espionage, data theft, monetary heists, and destructive malware operations." The following year, in March 2020, U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned two Chinese nationals, Tian Yinyin and Li Jiadong, for their role in helping Lazarus Group launder funds stolen in four separate cryptocurrency exchange hacks between 2017 and 2019. In this latter designation, 20 cryptocurrency addresses associated with sanctioned entities were added as identifiers.

Nation State Actors: Venezuela

Venezuela is suffering through one of the worst economic crises in modern history. In 2020, the annual inflation rate reached 6,500%. Under these circumstances, cryptocurrency has taken on an important role in Venezuela's economy. Many Venezuelans rely on cryptocurrency to receive remittances from abroad and preserve their savings against hyperinflation. At the same time, Venezuela's contested government, led by OFAC-sanctioned Nicolas Maduro and known for its corruption and human rights abuses, has launched its own cryptocurrency projects it claims will mitigate poor economic conditions for its citizens. However, officials have also stated that bypassing sanctions — a point of concern around cryptocurrency for the U.S. and its allies — is a key goal of these projects.

In 2018, the Venezuelan government started the Petro: a national cryptocurrency said to be backed by the country's oil reserves. In March 2018, then-President Trump issued Executive Order 13827, banning U.S. persons from transacting in the Petro. While the goal of the project is ostensibly to combat the currency devaluation hurting Venezuela today, government officials have also stated that evading sanctions is another goal. In addition to creating the Petro, the Maduro regime also gave seven cryptocurrency exchanges permission to operate in the country, their goal being to facilitate the exchange of the Petro so that it can circulate in the global cryptocurrency economy. These exchanges aren't limited to the Petro, of course — just like any other exchange, users can buy and sell popular cryptocurrencies like Bitcoin. In addition to the cryptocurrency exchanges, Caracas recently got its first Bitcoin ATM. The exchanges and Bitcoin ATM represent a risk of sanctions evasions, as individuals connected to the Maduro regime could theoretically use them to receive transfers from citizens of the U.S., E.U., or other jurisdictions that have implemented Venezuela-related sanctions.

Malicious Cyber-Enabled Actors

OFAC has sanctioned malicious cyber-enabled actors, including ransomware developers and attackers. Because of this, victims and financial intermediaries who facilitate ransomware payments on their behalf should be aware that making ransomware payments to sanctioned actors could be a violation. Ransomware victims may be forced to choose between paying the ransom and possibly suffering an additional penalty in the form of an OFAC violation, or not paying the ransom and suffering the loss of their data and the resulting financial costs of business disruption, or even death in the event that hospitals are attacked.

Ransomware payments increased in 2020, and are on pace to grow again in 2021. We are aware of ransomware strains related to sanctioned entities that have very likely rebranded, changing the ransomware names to obfuscate their connection to sanctions so that victims will continue to make ransom payments. We may see increases in ransomware payments with sanctions risk, if emerging strains receiving payments are connected to potential sanctions nexuses, or if OFAC designates additional ransomware groups. For instance,

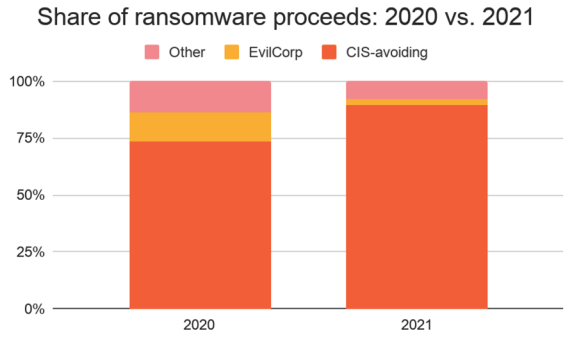
we've noticed that some Iranian ransomware strains have resurfaced under new names to disguise their connections to organizations and individuals with sanctions risk. It is therefore imperative that ransomware victims and those assisting them conduct due diligence using blockchain analytics to ensure that they are not violating sanctions should they choose to pay ransom.

Many ransomware strains are associated with sanctioned cybercriminal groups based in or affiliated with Russia, such as the sanctioned group Evil Corp, whose leadership reportedly has ties to the Russian government. Generally speaking, cybercriminals affiliated with Russia and other Russian-speaking countries in the Commonwealth of Independent States (CIS) — an intergovernmental organization of former Soviet countries — have been among the most prolific in the world. Russian-affiliated services received more cryptocurrency from illicit addresses than those in any other country, suggesting that Russian-affiliated cybercriminals are some of the biggest financial beneficiaries of cryptocurrency-based crime. Much of this activity is driven by Hydra, a Russia-based Darknet market, which, in addition to drugs, sells stolen data that can be useful to ransomware attackers.

In 2021, ransomware strains associated with Russia and other CIS countries are accounting for a larger share of overall ransomware activity. We show this on the graph below by comparing activity in 2020 and 2021 for two categories of ransomware strains:

- Strains associated with Evil Corp.
- Strains with code that prevents encryption if the ransomware detects the victim's operating system is located in a CIS country, labled "CIS-avoiding" in the below graph. These strains can generally be assumed to have originated in Russia or other CIS countries.

The numbers are clear: Taken together, these ransomware strains are accounting for more activity in 2021 compared to 2020.



Please note: This graph reflects the total amount of ransomware activity accounted for by the ten most prolific strains in 2020 and 2021. While this excludes many individual strains, it still reflects the majority of activity in both years.

In 2020, roughly 86% of ransomware proceeds studied could be attributed to ransomware strains that are either associated with Evil Corp or are designed to avoid CIS countries. So far in 2021, that figure is at 92%.

Transnational Criminal Organizations

We see a number of transnational criminal organizations (TCOs) exploiting cryptocurrency as a method of money laundering. This includes designated Mexican TCOs like the Cartel de Jalisco Nueva Generacion (CJNG) and the Sinaloa Cartel, which have turned to cryptocurrency to launder their illicit proceeds. In the past two years, OFAC has continued levying sanctions against these types of organizations, and has taken the step of listing their associated cryptocurrency addresses as identifiers in the designations.

In August 2019, OFAC announced sanctions against three Chinese nationals and the Zheng drug trafficking organization (DTO) for manufacturing and distributing hundreds of controlled substances, including fentanyl analogues, which they sold online. In the designation, 12 cryptocurrency addresses were included as associated identifiers. The Zheng DTO laundered their illicit proceeds using cryptocurrencies and, according to OFAC, "transmitted drug proceeds into and out of bank accounts in China and Hong Kong, and bypassed currency restrictions and reporting requirements." According to the Department of Homeland Security, the group was responsible for shipping fentanyl analogues and 250 other drugs to at least 25 countries and 37 states and the drugs sold by the group directly led to the fatal overdoses of two people in Akron, Ohio.

In December 2020, OFAC designated Wan Kuok Koi, aka "Broken Tooth," as well as three entities owned or controlled by him. According to OFAC, Wan "is a member of the Communist Party of China's (CCP) Chinese People's Political Consultative Conference, and is a leader of the 14K Triad, one of the largest Chinese organized criminal organizations in the world that engages in drug trafficking, illegal gambling, racketeering, human trafficking, and a range of other criminal activities." Wan was designated for corruption related to government contracts, bribery, and the expropriation of private assets for personal gain. Wan's World Hongmen History and Culture Association, which was also designated in this action, has spread across Southeast Asia, establishing a powerful business network involved in real estate, a security company specialized in protecting Belt and Road Initiative investments, and even the development and launching of cryptocurrencies. OFAC noted that Wan's activities meet "a pattern of overseas Chinese actors trying to paper over illegal criminal activities by framing their actions in terms of China's Belt and Road Initiative (BRI), the China Dream, or other major initiatives of the CCP." The Chinese enterprises behind the BRI projects, like Wan's, are often linked to criminal networks, and engage in money laundering using casinos and cryptocurrencies.

Challenges and Successes Under the Current Sanctions Regime

While we have seen sanctions have an impact against those exploiting cryptocurrencies and those seeking to use cryptocurrencies to evade sanctions, there is no denying that there are some challenges associated with the use of cryptocurrency to evade sanctions. As with any new technology, there is a learning curve. Investigators have had to develop the skills, tools, and capabilities necessary to go after these criminals. This sort of development takes time and money and requires agency leaders to prioritize these resources and efforts. Investigative techniques, training, and domain knowledge within the U.S. Government must continue to advance in line with the evolving technologies and the tactics deployed by bad actors attempting to abuse the digital financial ecosystem.

Financial screening and KYC checks can also pose a challenge for cryptocurrency exchanges. As the SES case underscores, even if exchanges have strong compliance regimes, there exist criminal groups willing to sell fake documents that allow illicit actors to pass KYC checks. These fraudulent identification documents, which can be enhanced with photo editing and deepfake video technology, can be used during the digital onboarding process to bypass sanctions screening. Chainalysis has begun to map out at least 50 other vendors like SES that provide fraudulent identity documents used during the digital onboarding process. While this challenge is not unique to cryptocurrency exchanges — there are an increasing number of online banks that must also confront this issue — it's vital that cryptocurrency businesses recognize this threat and adopt rigorous compliance measures to ensure their platforms aren't abused by those looking to skirt identification requirements to evade sanctions.

In addition, there are no comprehensive, international standards for digital identification documents, though some countries have proposed legislation to change that. That lack of standards has created a global cybersecurity risk. Whether they fall into the synthetic or stolen category, fake digital identity documents allow cybercriminals — including nation state threat actors — to abuse cryptocurrency businesses by skirting their compliance processes and evading bans put in place to prevent money laundering and terrorist financing. As cryptocurrency and other digital payments systems continue to grow, the Financial Action Task Force (FATF) has recognized the problem and called for a more standardized digital identification system. The shutdown and sanctioning of SES reinforces the need for such measures.

In spite of these challenges, there have been clear successes in this area. FinCEN's 2013 guidance clarified that cryptocurrency exchanges must register as MSBs and maintain compliance programs in the United States. The 2015 initiative to include Malicious Cyber-Enabled designations and the 2018 initiative to include digital currency addresses as identifiers associated with designated individuals or entities have both been impactful. Using blockchain analysis, Chainalysis can see the effectiveness of including digital currency addresses as identifiers in designations. Our data demonstrates that after digital currency identifiers are included, little to no more money flows to these addresses, indicating the positive impact of blacklisting wallet addresses. The figure below demonstrates this.

Chart Showing Impact of OFAC Including "Digital Currency Addresses" As Identifiers in Designations of Individuals and Entities

Designating body	Sanction type	Sanctioned Entity	Sanction date	Cryptocurrency value received pre-sanction	Cryptocurrency value received post-sanction
OFAC	SDN	Anton Nikolaeyvich Andreyev	9/10/2020	$1,205.07	$0.00
OFAC	SDN	Danil Potekhin (ETH)	9/16/2020	$2,047,908.63	$0.00
OFAC	SDN	Danil Potekhin (BTC)	9/16/2020	$5,023,874.52	$0.00
OFAC	SDN	EnExchanger	11/28/2018	$1,219,123.55	$0.98
OFAC	SDN	Fujing Zheng	8/21/2019	$23,300.02	$1.21
OFAC	SDN	Iranvisacart	12/4/2018	$2,974,970.15	$6.66
OFAC	SDN	Mujtaba Ali Raza	4/20/2021	$9,128.03	$0.00
OFAC	SDN	Secondeye Solution	4/15/2021	$130,878.61	$0.00
OFAC	SDN	Xiaobing Yan	8/21/2019	$1,057,546.71	$7.79

Two bureaus within the U.S. Department of the Treasury– the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN)– have issued advisories related to facilitating ransomware payments and the sanctions risk that this poses. OFAC has also taken action against cryptocurrency exchanges that have violated sanctions. In December 2020 and February 2021, respectively, OFAC entered into settlements with cryptocurrency exchanges BitGo and BitPay for violations of multiple sanctions programs.

Recommendations for Ways to Improve the Current Sanctions Regime with Regards to Cryptocurrency

I would like to provide some recommendations for ways to improve the efficacy of the current sanctions regime with regards to cryptocurrency. These include 1) encouraging collaboration and information sharing with international partners, 2) increasing public-private partnerships, 3) increasing OFAC's resources to support more comprehensive targeting and designations of individuals, organizations, and services that facilitate sanctions evasion using cryptocurrency, and 4) the creation of a National Cryptocurrency Targeting Center to improve cross-agency collaboration to combat the illicit use of cryptocurrencies.

Recommendation 1: Encourage Collaboration and Information Sharing with International Partners

Collaboration and information sharing with our international partners is critical in this space and concerted efforts to improve international partnerships should be made. Increased cross-border cooperation between law enforcement agencies can go a long way towards mitigating sanctions evasion and other illicit uses of cryptocurrency, such as cryptocurrency exchange hacks and ransomware attacks. If financial intelligence units (FIUs) around the world can swiftly share the information they get, they may be able to freeze funds before illicit actors are able to move them to a mixer or low-KYC exchange.

Additionally, OFAC is currently the only sanctioning body that lists digital currency addresses. There is an opportunity to work with other international sanctioning bodies to help them initiate similar efforts. This would improve the impact of these sanctions. As our data demonstrates, when OFAC does include a digital currency address as an identifier for a sanctioned individual or entity, there are rarely future payments to that address. The inclusion of these identifiers is incredibly effective and should be increased. The more sanctions that are levied that include these sorts of identifiers, the more difficult it will be for these malicious actors to operate.

Recommendation 2: Increase Public-Private Partnerships

We recommend increasing and improving public-private partnerships in this space. The more information that is shared, the better able we are to combat illicit activities like sanctions evasion. There have been a number of legislative proposals, including the "Combating Illicit Finance Public-Private Partnerships Act" and proposed OFAC Exchange Act, which would improve public-private information sharing opportunities among Federal agencies, financial institutions, and private sector experts in banking, national security, and law enforcement. We believe that these sorts of partnership proposals would be effective in improving the U.S. response to sanctions evasion, money laundering, terrorist financing, and other financial crimes.

Recommendation 3: Increase OFAC's Resources to Support More Comprehensive Targeting

We would also encourage more designations of illicit actors and those who facilitate their criminal activities. In order to enable this, OFAC's funding and resources should be increased. This would support their efforts to engage in more comprehensive targeting and designations of individuals, organizations, and services that facilitate sanctions evasion using cryptocurrency. We know that in the case of malicious cyber actors, such as ransomware attackers, bulletproof hosting services, VPN providers, Darknet markets, and/or online fraud shops are critical to their success. OFAC should designate more facilitators, much as they did with SES for providing fraudulent identification documents to malign foreign actors. OFAC routinely designates facilitators of terrorists and TCOs, and should employ the same tactic with those who enable malicious cyber actors. Since the

components of ransomware are often sold on Darknet markets and online fraud shops, OFAC should also consider designating those groups.

Recommendation 4: National Cryptocurrency Targeting Center

Finally, while there are a number of law enforcement agencies that have been building up their blockchain analysis capabilities, these efforts have been siloed and largely uncoordinated. To increase collective impact and achieve large-scale objectives, the U.S. should consider the creation of a National Cryptocurrency Targeting Center. This would house representatives from many U.S. government agencies, working together to combat the illicit use of cryptocurrencies. The center could also provide training opportunities to the member agencies to raise awareness of what indicators exist in an investigation to indicate that cryptocurrency might be being exploited, publish guides and reports on trends and how criminal techniques are changing, as well as best practices in investigations, and serve as an information sharing venue for law enforcement.

Conclusion

In closing, we applaud your efforts to improve the effectiveness of our sanctions. Cryptocurrency and blockchain technology offer the promise of bringing more people into the global financial system, but it's important to ensure malicious actors aren't abusing that promise. I therefore encourage you to consider the impact any potential legislation could have on technical innovation. While adversaries have quickly embraced cryptocurrency, sometimes for illicit purposes, we have found that not only are the vast majority of cryptocurrency transactions legitimate, the percentage of illicit use of cryptocurrencies is dropping. This may be due to greater awareness about blockchain analysis, which provides insights into transactions and trends that are invaluable to investigators. This sort of visibility is not possible with other forms of value transfer. We hope to see the United States lead on the cryptocurrency front — because if we don't, others will. Thoughtful regulation that promotes American innovation while supporting law enforcement and financial regulators will be crucial for the United States to maintain its position as the leader of the global financial system.

# # # # #

Testimony of

Jeffrey W. Taliaferro
Professor of Political Science, Tufts University
Former Fellow, Woodrow Wilson International Center for Scholars (AY 2017-2018)

before the

House Committee on Financial Services

Subcommittee on National Security, International Development and Monetary Policy

Virtual Hearing on

"Schemes and Subversion: How Targets of Sanctions Undermine and Evade Sanctions"

2:00 PM EDT, Wednesday, June 16, 2021

Thank you, Chairman Himes and Ranking Member Barr, for the opportunity to testify this afternoon. It is a privilege to speak to this Subcommittee and to be on this distinguished panel of witnesses.

Let me state at the outset that I am a scholar of international security. I am neither an economist nor a scholar of political economy. My scholarship and teaching primarily deal with United States national security and intelligence, the grand strategies of the great powers (both past and present), alliance politics, nuclear proliferation, and more recently cybersecurity.

My most recent book examines the nuclear proliferation disputes between the United States and four vulnerable and sometimes obstreperous allies—Israel, Pakistan, South Korea, and Taiwan—over a thirty-year period from roughly 1961 to 1990. Specifically, I sought to explain why and how different presidential administrations (from John F. Kennedy to Ronald Reagan) tried to balance the strategic objectives of containing the growth of the Soviet Union's influence in the Middle East, South Asia, and the Middle East, on the one hand, and forestalling US allies from developing independent nuclear weapons capabilities, on the other hand. In several cases, administrations worked closely with other allies to impose controls on the export of dual-use technologies, to uncover nuclear smuggling rings, and to trace illicit financial transactions. On a few other occasions, administrations threatened to suspend conventional arms transfers and civilian nuclear cooperation to coerce the ally's compliance with nonproliferation demands.[1]

My fellow witnesses are more qualified to testify about the design and implementation of

[1] Jeffrey W. Taliaferro, *Defending Frenemies: Alliance Politics and Nuclear Nonproliferation in US Foreign Policy* (New York: Oxford University Press, 2019).

sanction regimes; about the various strategies and newer tools that targeted actors employ to evade or undermine sanctions; and to offer recommendations for how the Congress and the executive branch might craft more effective sanctions in the future. Instead, my role on this witness panel is to provide a broad overview of the geopolitics of the United States' use of sanctions against a variety of actors—great powers, regional powers, minor powers, corporations, non-state actors, and individuals—as well as the geopolitical implications of the evasion or subversion schemes employed by those targeted actors and their allies.

Economic and trade sanction have long been an important non-kinetic tool of coercive diplomacy among states. The Office of Foreign Asset Control (OFAC) in the US Department of the Treasury notes sanctions are based on "US 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."[2]

The primary aim of sanctions—whether unilateral or multilateral, targeted or comprehensive—is to induce a change in the cost-benefit calculations of the target, and thus a change in the target's behavior. The actual imposition of the sanctions must be contingent on the target's observable behavior and the coercer must have both the capability and the resolve to do so.[3] But as with other tools of statecraft, including kinetic force, the use of sanctions to secure a target's compliance with a coercer's demand is inherently difficult. There are no guarantees of coercive "success" even in disputes where the balance of material capabilities (power) clearly favors the coercer.[4] Nonetheless, the threat and imposition of sanctions can serve other political objectives.

Since the late 1940s, the United States has invested in security institutions, such as the UN Security Council and NATO, for several reasons.[5] These include: (1) to conserve is own material capabilities over the long-run by sharing the short-term costs of coercive diplomacy with other states; (2) to overcome domestic mobilization hurdles to participation through appeals to

---

[2] Office of Foreign Assets Control—Sanctions Programs and Information, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (accessed June 13, 2021)

[3] The foundational work on coercion theories remains Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966). For a good overview of the literature see Tamis Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* 3, no. 2 (2020): 94-109.

[4] For a concise summary of the myriad reasons why coercive success often proves elusive regardless of the tools of statecraft employed see Robert J. Art and Kelly M. Greenhill, "Coercion: An Analytical Overview," in Kelly M. Greenhill and Peter Krause, *Coercion: The Power to Hurt in International Politics* (New York: Oxford University Press 2018), pp. 18-19.

[5] Anders Wivel and T. V. Paul define international institutions as "associational clusters among states with some bureaucratic structures that create and manage self-imposed and other imposed-constraints on state policies and behavior." See "Exploring International Institutions and Power Politics," in Wivel and Paul, eds., *International Institutions and Power Politics: Bridging the Divide* (Washington, DC: Georgetown University Press, 2019), p. 8.

international legitimacy and claims that any burden will be shared by allies and partners; (3) to leverage the legitimacy of these institutions to generate domestic pressure in other countries for their participation; and (4) to assist in signaling intent to adversaries, as well as neutrals, which might prevent conflicts from escalating.[6]

Over the past thirty years, the United States has worked through the UN Security Council, NATO, and other institutions to create and enforce multilateral sanctions regimes against states such as Iraq, Iran, Serbia, Libya, Russia, China, and North Korea (among others), for each of the above-mentioned reasons. Since the 2010s, the United States, alongside allies and partners and often working through international institutions, has increasing employed targeted or "smart" sanctions—designed to impose costs on the elite and key supporters of the targeted regime while minimizing the pain felt by the state's general population.[7]

Additionally, the United States has unilaterally threatened and imposed sanctions against a variety of targets. There are at least two reasons for this. First, unilateral sanctions can signal to domestic constituencies that the Congress and/or the administration of the day takes a particular issue "seriously," or that they "intend to send a message," or that they are resolved "to do something," even if unilateral sanctions have little chance of inducing the target's compliance in the foreseeable future. Second, unilateral sanctions can signal to foreign audiences—allies and partners, neutrals, and especially adversaries—the degree of resolve on the part of the Congress or the administration regarding an issue.

The United States has increasingly relied on economic and trade sanctions as important tools of statecraft. Targeted entities have included a variety of states, terrorist organizations, international criminal syndicates, private companies, and individuals. These actors have long employed a variety of means to evade or subvert unilateral sanctions as well as the multilateral sanction regimes the United States helps organize and enforce.

My fellow witnesses will discuss some of the newer tools and technologies used to facilitate sanctions evasion, such as cryptocurrencies, Central Bank Digital Currencies (CBDCs), and ransomware. However, I would like to highlight how shifting geopolitical dynamics are making it more difficult for the United States to credibly threaten and enforce sanctions while also giving targets additional means and opportunities to evade and subvert them.

Having won the Cold War and pushed the crumbling Soviet Union out the ranks of the great

---

[6] Norrin M. Ripsman, "A Neoclassical Realist Explanation of International Institutions," in Anders Wivel and T.V. Paul, eds., *International Institutions and Power Politics*, pp. 45-50.

[7] For an overview of the scholarly debates over the efficacy of economic sanctions, in general, and of targeted (or "smart") sanctions, in particular see Daniel W. Drezner, "Economic Sanctions in Theory and Practice: How Smart Are They?" in Greenhill and Krause, eds., *Coercion: The Power to Hurt in International Politics*, pp. 251-270.

powers, United States emerged as the unipole in 1990-1991.[8] By definition, a unipolar international system has only one great power, a single state whose relative share of power—especially its extant military and economic capabilities—is too great to be counterbalanced in the near-term by any other state or possible combination of states. While preponderance does not give a unipole complete control over the external behavior of all other states, a unipole does face far weaker systemic constraints than those faced by the two superpowers in a bipolar system that existed during the Cold War or the several great powers in a multipolar system, such as the one that existed in Europe until World War II.[9] For better or worse, for two decades, weak systemic constraints and the availability of opportunities to further improve its strategic position afforded the United States wide latitude in the pursuit of foreign and national security policies.[10]

This extreme imbalance of power had several consequences relevant to the subject of today's Subcommittee hearing.

First, the United States imposed economic and trade sanctions on and even waged wars against recalcitrant states, such as Iraq, Serbia, Libya, and Afghanistan, and non-state actors, such as al Qaeda and later the Islamic State (or ISIS), with relative impunity.[11] No other state or coalition of states had the material capabilities to deter the United States. And when confronting state adversaries against whom the use of kinetic force would have been cost prohibitive, such as North Korea and Iran, the imposition of economic and trade sanctions became a preferred tool for successive administrations and the Congress.

Second, the US military's command of the global commons and ability to sustain prolonged military operations in distant regions, along with the United States' economic and technological dominance, gave various state and non-state actors an incentive to develop asymmetric strategies.[12] One such strategy is hybrid interference, defined as "the synchronized use of multiple non-military means of interference tailored to heighten divisions within target

---

[8] Joshua R. Itzkowitz Shifrinson, Rising Titans, *Falling Giants: How Great Powers Exploit Power Shifts* (Ithaca: Cornell University Press, 20180, pp.

[9] See G. John Ikennberry, Michael Mastanduno, and William C. Wohlforth "Introduction: Unipolarity, State Behavior, and Systemic Consequences," *World Politics* 61, no. 1 (2009): 1-27; Stephen M. Walt, "Alliances in a Unipolar World," *World Politics* 61, no. 1 (2009): 86-120; and Stephen G. Brooks and William C. Wohlforth, *World out of Balance: International Relations and the Challenge of American Primacy*. (Princeton: Princeton University Press, 2008).

[10] See Jeffrey W. Taliaferro, Steven E. Lobell, and Norrin M. Ripsman. "Introduction: Neoclassical Realism, the State, and Foreign Policy," in Steven E. Lobell, Norrin M. Ripsman and Jeffrey W. Taliaferro, eds., *Neoclassical Realism, the State, and Foreign Policy* (Cambridge: Cambridge University Press, 20090, pp. 1-41; and Norrin M. Ripsman, Jeffrey W. Taliaferro, and Steven E. Lobell, *Neoclassical Realist Theory of International Politics* (New York, NY: Oxford University Press, 2016), pp. 52-56.

[11] See Nuno P. Monteiro, *Theory of Unipolar Politics* (Cambridge: Cambridge University Press, 2014), pp. 144-178.

[12] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (2003): 5-46.

societies."[13] Hybrid interference employs a variety of state-controlled but non-kinetic tools "that are concealed to provide the divider with official deniability and manipulate targeted actors without elevating threat perceptions."[14] Such tools include clandestine diplomacy (e.g., covert assistance to opposition groups, criminal organizations, insurgents, and hackers), geoeconomics (e.g., the use of financial inducements and threats against select individuals or groups within the target state), and disinformation (e.g., the introduction of false or misleading information into the communication streams of the target state).

To date the most successful (and infamous) employment of hybrid interference directly targeting the United States was Russia's two-year long operation to sway the outcome of the 2016 presidential election.[15] Indeed, the clandestine employment of cybercriminal organizations and individual hackers by the foreign intelligence services of Russia, China, North Korea, and Iran, enable them to not only carry out hybrid interference campaigns targeting the United States, its allies, and strategic partners, but also to undermine various unilateral and multilateral sanctions. And all the while, the Russian, Chinese, North Korea, and Iranian governments can maintain plausible denial. Additionally, China has variously utilized its Belt and Road Initiative (BRI) development projects, the technology firm Huawei's dominance of the market in 5G network infrastructure, and disinformation campaigns on social media to drive wedges between the United States and various allies in Western Europe, South Asia, and East Asia.[16]

Third, the unipolar distribution of power itself, as well as the diplomatic, military, and foreign economic initiatives undertaken by the Bill Clinton, George W. Bush, Barak Obama, and Donald J. Trump administrations, created incentives and opportunities for targets and other disaffected actors to collaborate to evade or subvert US sanctions. For example, Russia under President Vladimir Putin, seized the opportunity to provide a lifeline to the embattled regime of Venezuela's president Nicolas Maduro by allowing the Russian oil company Rosneft to buy, transport, and sell Venezuelan crude oil. This arrangement allowed *Petróleos de Venezuela, S.A.* (PDVSA), and by extension Maduro's government and power base, to profit from the sale. Rosneft ended formal operations in Venezuela in March 2020 after two successive rounds of US sanctions targeting the subsidies which enabled the sale of crude.[17] But Rosneft sold its Venezuelan assets to a Russian state-owned company, thus giving Putin's government both a

---

[13] Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy." *International Affairs* 95, no. 2 (2019), pp. 255-275, at p. 262.
[14] Ibid., p. 256
[15] See Wigell, "Hybrid Interference"; and Benjamin Jensen, Benjamin, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (2019): 212-34.
[16] Weifeng Zhou and Mario Esteban, "Beyond Balancing: China's Approach Towards the Belt and Road Initiative." *Journal of Contemporary China* 27.112 (2018): 487-501.
[17] "Treasury Targets Additional Russian Oil Brokerage Firm for Continued Support of Maduro Regime," U.S. Department of the Treasury, March 12, 2020, https://home.treasury.gov/news/press-releases/sm937 (accessed June 15, 2021).

major stake in Venezuela's energy sector and strategic foothold in South America.[18]

Likewise, China has a long record of enabling North Korea to circumvent various UN Security Council sanctions aimed at coercing the surrender of its nuclear weapons. In December 2020, the US Department of State accused China of "flagrant violations" of its obligation to enforce UN sanctions citing evidence that Chinese firms not only continued to do business with North Korean officials and entities associated with the nuclear weapons program, but also helped North Korea launder money obtained through cyber threat in order to fund that weapons program.[19] There is evidence that China may have loosened its protective stance on North Korea in recent years, whether in response to diplomatic pressure from the United States during the Trump administration, North Korean long-range missile tests in 2017, changing Chinese perceptions of Kim Jong Un's regime, or some combination of all three.[20] Nevertheless, Chinese president Xi Jinping is not about to "abandon" North Korea by ordering rigorous compliance with nonproliferation sanctions. The survival of North Korea, which is inextricably tied to the survival of the Kim dynasty, is of paramount strategic importance to China.

Fourth, and finally, as the Biden administration's *Interim National Security Strategic Guidance* acknowledges, "the distribution of power across the world is changing, creating new threats."[21] The United States now faces two great power adversaries, a rising China and a revanchist Russia, as well as two regional power adversaries, Iran and North Korea. "Both Beijing and Moscow have invested heavily in efforts meant to check U.S. strengths and prevent us from defending our interests and allies around the world. Regional actors like Iran and North Korea continue to pursue game-changing capabilities and technologies, while threatening U.S. allies and partners and challenging regional stability."[22] All four states will seek more creative means to evade the various economic and trade sanctions the United States seeks to enforce. They will also continue to help their respective allies and clients to subvert or evade sanctions.

One would expect the Congress and the executive branch to redouble efforts at vigorous sanctions enforcement. But in this changing geopolitical landscape, it might also behoove policymakers to be bit reticent in imposing sanctions against various targets and to lower

---

[18] David L. Goldwyn, "Containing Russian Influence in Venezuela," The Atlantic Council, April 20, 2021, https://www.atlanticcouncil.org/blogs/energysource/containing-russian-influence-in-venezuela/ (accessed June 15, 2021). Also see John E. Herbst and Jason Marczak, "Russia's intervention in Venezuela: What's at stake?" The Atlantic Council, September 12, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/russias-intervention-in-venezuela-whats-at-stake/ (accessed June 15. 2021).

[19] David Brunnstrom, "U.S. accuses China of 'flagrant' N. Korea violations, offers $5 million reward," Reuters, December 1, 2020, https://www.reuters.com/article/usa-northkorea-china-idUSKBN28B540 (accessed June 15, 2021).

[20] Wenxin Li and Ji Young Kim. "Not a Blood Alliance Anymore: China's Evolving Policy toward UN Sanctions on North Korea." *Contemporary Security Policy* 41, no. 4 (2020): 610-31.

[21] Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 3, 2021) https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

[22] Ibid, p. 7

expectations about what coercive (economic) diplomacy can achieve vis-a-vis such determined adversaries.

IVAN A. GARCES

PRINCIPAL & CHAIR, RISK ADVISORY SERVICES

KAUFMAN ROSSIN

Response to Questions for the Record

from Congressman Jim A. Himes,

Chair of the

COMMITTEE ON FINANCIAL SERVICES

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT AND MONETARY POLICY

UNITED STATES HOUSE OF REPRESENTATIVES

Virtual Hearing on

"Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes"

June 16, 2021

I. Introduction

On June 16, 2021, the United States House of Representatives Committee on Financial Services, Subcommittee on National Security, International Development and Monetary Policy convened a virtual hearing entitled, "*Schemes and Subversion: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes.*" After the hearing, Chairman Himes submitted Questions for the Records to the participating witnesses.

Chairman Himes, thank you for your Questions for the Record. This document provides my responses to those Questions for the Record that were addressed to me.

II. Beneficial Ownership Database

Question. This body passed the landmark anti-money laundering and national security legislation, the Anti-Money Laundering Act of 2020 and the Corporate Transparency Act, on January 1st of this year. In fact, both of those laws started in this committee with bipartisan support. They make a number of changes to the nation's anti-money laundering regime, including the addition of a national registry of beneficial ownership information for firms that are not already reporting that information to other authorities. Congress is looking at funding for this database and the other mandates in these laws, now and in the FY2022 budget.

a. Could you please share how being able to understand the true and beneficial ownership behind front companies and anonymous shell companies will help detect and deter sanctions evaders, including kleptocrats, drug dealers, or terrorists?

Response. Shell and front companies provide sanctions evaders and malign actors a vehicle to obscure their identities and mask transactions to exploit international trade and financial systems to further their nefarious activities. Given the anonymity provided, sanctioned individuals and malign actors utilize front and shell companies to disguise transactions, circumvent anti-money laundering and sanctions compliance efforts, and stymie investigations.

Understanding the true and beneficial ownership of legal entities assists financial institutions in meeting their customer due diligence requirements. Knowing who ultimately owns and controls the legal entities can enhance new customer acceptance and onboarding procedures;

customer risk assessments; monitoring of accounts for suspicious or sanctioned activity; and quality of suspicious activity reports.

Sanctions evaders and malign actors often layer their activity through complex structures across jurisdictions with one shell company owned by another. Such complex organizational structures can frustrate and prolong investigations. Knowing the true and beneficial owners behind front and shell companies can assist government agencies and law enforcement in identifying the natural persons responsible and tracing relationships between seemingly unrelated entities.

The passage of the Corporate Transparency Act and the implementation of a national beneficial ownership registry brings much needed corporate transparency by requiring legal entities to report the natural persons who ultimately own or control them, thus making it harder for sanctions evaders and malign actors to use shell companies to carry out their nefarious activities.

III. Traditional Methods of Sanctions Evasion

Question. One of the most common evasion techniques is the use of front or shell companies.

a. Can you comment on how sanctions targets use front companies and anonymous shell companies to evade sanctions, perhaps offering some illustrations of those cases?

Response. As a result of the ease of creation and anonymity provided, sanctions evaders utilize shell companies to conceal their identity, disguise transactions and evade detection. Sanctions evaders often layer their activity through complex structures across jurisdictions. Sanctions evaders utilize shell companies to engage in prohibited transactions, establish accounts and gain access to international financial systems. A few recent public cases involving shell companies follow:

> **Manhattan U.S. Attorney Announces Forfeiture of Oil Tanker Used to Violate Sanctions Against North Korea** ***(July 30, 2021)***
>
> The *M/T Courageous*, a 2,734-ton oil products tanker will be forfeited due to its involvement in the illicit delivery of petroleum products through transfers with vessels in North Korea and to Nampo, a port city in the South Pyongan Province of North Korea. The tanker's alleged owner and operator, Kwek Kee Seng, a Singaporean national, is facing criminal charges of conspiracy to evade economic sanctions on North Korea and conspiracy to commit money

laundering. According to the complaint for forfeiture, Kwek and his co-conspirators processed U.S. dollar payments through domestic correspondent accounts in New York utilizing shell companies. As part of the scheme, Kwek utilized Courage Maritime SA, a shell company incorporated in Panama and New Eastern Shipping, a Chinese company serving as the straw purchaser, to conceal the fact that these transactions were conducted to purchase the *M/T Courageous*, oil and finance related services including registration fees, ship materials and crew salaries. Between July 8 and July 17, 2019, nine separate U.S. dollar payments totaling $580,000 were made by New Eastern Shipping for the purchase of the *M/T Courageous*. However, a different entity, Visson Electronics Co. Limited, was identified as the originator of the purchase transactions, not New Eastern Shipping, the straw purchaser serving as a front to purchase the *M/T* Courageous for use in the DPRK Shipping Scheme. Invoices for services related to the *M/T Courageous* were billed to Courage Maritime S.A., the vessel's alleged owner while payments were made by front company, Swanseas Port Services, owned by Kwek. Further, Kwek and his co-conspirators allegedly disguised location information for four months and conducted ship-to-ship fuel transfers to vessels such as the *Saebyol*, an OFAC-designated North Korean vessel on the open sea to conceal the counterparties involved. The *Courageous* was ultimately seized by Cambodian authorities in March 2020.[1]

Justice Department Seeks Forfeiture of More than $20 Million in Assets Relating to Unlawful Use of U.S. Financial System to Evade and Violate Iranian Sanctions *(June 3, 2020)*

From 2011 to 2014, Kenneth Zong, a U.S. citizen, and three Iranian nationals allegedly engaged in fictitious and fraudulent transactions designed to unlawfully convert and remove Iranian owned funds in a South Korean financial institution, totaling approximately $1 billion USD. The group's

[1] https://www.justice.gov/usao-sdny/press-release/file/1389271/download.

actions appear to have been an attempt to evade the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR). According to the complaint for forfeiture, Zong and his co-conspirators represented to the Industrial Bank of Korea (IBK) that Anchore had sold hundreds of millions in permitted goods and services (i.e., marble tiles, construction materials) to Iran (i.e., Farsoodeh and Partnership). Anchore, an apparent front company, was registered in Seoul, South Korea and owned by Zong. Although there were no actual transactions between Anchore and Iran, Zong and co-conspirators presented IBK with fraudulent purchase and sale documents to support the request for IBK to transfer funds from the Central Bank of Iran's account to Anchore's account which were ultimately wired to several shell company accounts in jurisdictions such as the UAE. The Department of Justice was able to trace $20 million in funds to the down payment for the purchase of a Sheraton Hotel in Tbilisi, Georgia in 2011 and 2012.[2]

Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions *(July 23, 2019)*

Ma Xiaohong (Ma), her Chinese company, Dangdong Hongxiang Industrial Development Co. Ltd. (DHID) and three company executives were indicted for violating the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA and defraud the U.S. and conspiracy to launder monetary instruments. According to the indictment, from 2009 to 2015, the defendants are charged with utilizing more than 20 front companies established in offshore jurisdictions such as the British Virgin Islands, Seychelles, Hong Kong, Wales, England and Anguilla to facilitate illicit financial transactions. Many of the front companies shared an address in the British Virgin Islands or Hong Kong. The defendants allegedly opened accounts for these entities in 12 Chinese banks that maintained correspondent accounts in the U.S. The indictment suggests that the defendants likely knew that the transactions would

[2] https://www.justice.gov/opa/press-release/file/1282836/download

have been blocked if the correspondent banks knew that they were funded by parties in North Korea. These illicit financial transactions were conducted for the benefit of sanctioned North Korean entities involved in the proliferation of weapons of mass destruction. DHID would utilize front companies to give the appearance of legitimate sales of goods such as refined sugar and fertilizer with the ultimate objective of transferring funds to Korea Kwangson Banking Corporation (KKBC). Since these transactions are alleged to have been financed by KKBC, an OFAC SDN, the front companies were utilized to hide KKBC's presence from the U.S. correspondent banks and to prevent the transactions from being blocked. The indictment further stated that at the time there was no evidence that any of the defendants applied for, received, or possessed a license or authorization from OFAC to engage in transactions with a U.S. person or within the U.S. for the benefit of KKBC.[3]

b. Are there additional steps that Congress needs to complement the upcoming FinCEN registry on beneficial ownership?

Response. The Corporate Transparency Act and implementation of the FinCEN beneficial ownership registry is a step in the right direction, creating much needed corporate transparency. For the registry to be effective and highly useful to government agencies, law enforcement, and financial institutions it must be accurate and reliable as a central source of beneficial ownership information. Currently, it appears that the beneficial ownership reporting requirement relies on the submission of the reporting entity. Steps should be taken to ensure the accuracy and reliability of the beneficial ownership information provided to FinCEN, such as a certification requirement at registration and ongoing on a periodic basis. FinCEN should also consider implementing risk-based procedures for verifying beneficial ownership information submitted by reporting entities which would add to the accuracy and reliability of the registry. Given the electronic means in which beneficial ownership information is submitted and stored, some of the aspects of the verification can be automated. The FinCEN registry should also be scanned periodically against

[3] https://www.justice.gov/opa/press-release/file/1186081/download

sanctions lists and lists of known or suspected malign actors. Such information should be accessible to government agencies, law enforcement and financial institutions on a timely basis.

IV. Other Industries that are Targets of Abuse by Sanctions Evaders

Question. Designated individuals such as oligarchs or foreign officials often manipulate various avenues to evade American sanctions. We hear sometimes, too, that banks are generally in a good position vis a vis sanctions evasion, at least having deeply embedded and sophisticated systems and processes to look for evaders and their schemes. But what about the "others," meaning other industries that are targets of abuse by sanctions evaders?

a. Based on past cases and evaluations of risk, what areas of trade (i.e., trade industries), if any, are most vulnerable to sanctions evasion and why?

Response. Prior to the passage of the Corporate Transparency Act, financial institutions generally carried the burden of identifying and verifying the beneficial owners of legal entities under customer due diligence requirements. Financial institutions have, for some time, implemented systems to monitor, detect, reject, block and report sanctioned activity. They are also subject to regular examinations and enforcement by supervisory agencies. However, financial institutions can't be expected to connect all the dots. Broader private sector involvement is needed, as well as evolution of sanctions compliance programs, supervision and enforcement in industries susceptible to OFAC sanctions risk, such as the maritime industry, high value real-estate and luxury items, art, precious metals and digital currencies. These industries, which are largely unregulated, are particularly susceptible to sanctions evasion considering the ability to convert high-value transactions and the use intermediaries and shell companies to conceal the true beneficial owners and transaction counterparties.

V. Conclusion

Thank you again for your Questions for the Record. I would be happy to respond to any additional questions the members of this Subcommittee may have for me.

* * * * * * * *

Chainalysis

Responses to Representative Himes' Questions for the Record
Jesse Spiro, Chief of Government Affairs
Chainalysis

House Financial Services Committee
Subcommittee on National Security, International Development and Monetary Policy

Hearing on
Schemes and Subversion:
How Targets of Sanctions Undermine and Evade Sanctions Regimes

Wednesday, June 16, 2021

1. ***Mr. Spiro,*** *a report by your firm, Chainalysis, says that 15% of all ransomware payments made in 2020 carried a risk of sanctions violations. Echoing that concern, OFAC and FinCEN each issued an advisory last October to warn about ransomware and ransom payments. Your firm has also calculated that the total amount paid by ransomware victims increased by 344% from 2019 to 2020 to reach nearly $350 million worth of cryptocurrency – and that's just a figure comprised of the known ransoms.*

Chainalysis recently updated our statistics related to ransomware payments. It remains true that 15% of all ransomware payments Chainalysis identified made in 2020 carried a risk of sanctions violations. From 2019 to 2020, there was a 344% increase in ransomware payments to over $416 million worth of payments. As of July 2021, this year has already seen victims pay over $210 million to ransomware attackers. This demonstrates that the issue of ransomware continues to be an important one and we are glad that Congress and this Administration are taking it seriously.

   a. *What else do we learn about the bad actors or their facilitators when we trace the various cryptocurrencies that are typically paid in ransomware cases?*

Many cryptocurrencies, like bitcoin, which is still favored among ransomware attackers, are based on a decentralized blockchain, allowing for investigators to trace transactions through the blockchain. Using blockchain analysis tools like the ones that Chainalysis builds, law enforcement can trace the ransom paid in cryptocurrency to its cashout point at cryptocurrency exchanges. In the United States, cryptocurrency exchanges are regulated and required to register as money service businesses with FinCEN, maintain AML/CFT programs and collect Know Your Customer (KYC) information from their customers. Cryptocurrency exchanges are also regulated in many other jurisdictions, and have AML/CFT requirements with which to comply.[1] This means that law enforcement can serve cryptocurrency exchanges with legal process to obtain KYC and any other relevant information. In their response to legal process, a cryptocurrency exchange will provide any identifying information that they have related to the cryptocurrency address, such as name, address, and government identification documentation to law enforcement, allowing law enforcement to further their investigation. Not only do exchanges play a

[1] According to the Financial Action Task Force's *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*, 52 of the 128 FATF jurisdictions surveyed had implemented regulations for cryptocurrency exchanges and another 26 were in the process of doing so via legislative or rulemaking process.

role, but ransomware actors deposit funds at services that further their operations such as domain registration or cloud storage hosting and these services. They too can play a role in identifying threat actors.

In addition to the ability to trace the illicit cryptocurrency to a cash out point, blockchain analysis provides the ability to develop valuable intelligence about ransomware attackers. Using blockchain analysis tools, investigators can identify: the ransomware administrators, who develop the malware and their affiliates, who conduct the attack, based on the percentage of proceeds that each receives. Investigators can also determine how much revenue each has earned. Blockchain forensics can sometimes confirm connected variants that have rebranded or changed names in an attempt to obfuscate connections to sanctioned entities. Blockchain analytics is also used to identify which hosting platforms they are using, which VPNs they are using, changes in tactics, techniques and procedures, and which forums they are advertising on. All of this information will lead investigators to valuable clues that may allow them to identify the attackers, even if they do not cash out their illicit proceeds. It can also allow law enforcement to prioritize the most damaging attackers, as well as to provide important information to the private sector that may help them prevent ransomware attacks.

b. *Do you have recommendations on how to minimize sanctions-evasion risk in ransomware payments based on those findings?*

Given the recent increase in ransomware attacks, as well as their potentially devastating impact, Chainalysis believes it is important to enact meaningful policies to deter, detect, and disrupt ransomware. The foundation of these policies must be a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks. We applaud recent positive efforts spearheaded by the White House, including President Biden's May 12 Executive Order aimed at improving U.S. cybersecurity and the July 15 announcement of a new ransomware task force that will bring together federal agencies in a cross-government effort to defend against and investigate ransomware attacks. We are also encouraged by reports that members of Congress plan to introduce legislation that would require companies, including critical infrastructure operators, to report ransomware attacks to the government. Having access to timely and comprehensive information is critical to the success of investigators in these cases. To this end, we believe that the recent launch of the U.S. Government's stopransomware.gov website will serve as an important resource to prevent ransomware attacks and improve the response to ransomware attacks when they do happen.

Additional recommendations that Congress should consider when determining future legislation and strategies necessary to combat ransomware include improving public-private partnerships and ensuring adequate funding, staffing, training, and resources to investigate and combat ransomware attacks. Ransomware and other cyber-related crimes have challenged the traditional investigative methods employed by law enforcement. Investigators have had to develop the skills, tools, and capabilities necessary to go after ransomware attackers. This takes time and money and requires agency leaders to prioritize these resources and efforts, such as blockchain analysis tools and training. At the same time, criminals continue to develop new tactics and techniques, so it is important to have public-private partnerships that allow for the faster development of tools and allow for law enforcement to keep up with criminals. Continuing to ensure that investigators have the tools and resources necessary to conduct effective investigations will be a critical component in the fight against ransomware.

In addition, in order to disrupt the existing ransomware ecosystem, public-private information sharing could be improved and incentivized. Information is not currently shared in a consistent or reliable manner, and it does not always reach a broad enough audience. There is also currently underreporting of ransomware events, which obfuscates the true scope of the issue and means that law enforcement does not have all of the necessary information to prioritize and investigate ransomware events. The development of information sharing networks, both within the government, and between the government and the private sector, would improve the quality and volume of information about ransomware incidents. It may be worth considering a standard format for ransomware incident reporting to promote consistency, or providing suggested fields to include, such as cryptocurrency wallet addresses, transaction hashes, and ransom notes. Incentives could be put in place to facilitate information sharing between the private sector, financial institutions and money service businesses, law enforcement, and regulators.

2. ***Mr. Spiro**, what tools might be needed to stay ahead of activities with the intent to evade sanctions as the world economy moves further into virtual assets, digital and crypto currencies, non-fungible assets or tokens (NFT), or other emerging asset developments?*

Blockchain analysis tools, like the ones that Chainalysis develops, are an important tool in monitoring for illicit activity in cryptocurrency transactions. Blockchain analysis helps people interpret public blockchain ledgers and understand which real-world entities are transacting with each other. For example, using blockchain analysis, Chainalysis can show that a given transaction took place between two different cryptocurrency exchanges, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. Using this technology, government agencies can gain transparency into blockchain activity in ways that aren't possible in traditional finance. Likewise, with transaction monitoring, cryptocurrency exchanges and financial institutions can flag high-risk activity in real-time and fulfil their regulatory obligations.

   a. *What problems or threats might be posed by the possibility of a foreign government issuing or backing virtual assets?*

There are a number of potential threats to be considered related to foreign governments issuing virtual assets. In 2018, the Venezuelan government created the Petro, a national cryptocurrency said to be backed by the country's oil reserves. In March 2018, then-President Trump issued Executive Order 13827, banning U.S. persons from transacting in the Petro. While the goal of the Petro project is ostensibly to combat the currency devaluation hurting Venezuela today, government officials have also stated that evading sanctions is another goal. The Maduro regime gave seven cryptocurrency exchanges permission to operate in the country, their goal being to facilitate the exchange of the Petro so that it can circulate in the global cryptocurrency economy. Individuals connected to the Maduro regime could use these exchanges to receive transfers and evade sanctions.

Many countries are also researching or developing central bank digital currencies (CBDCs). For example, China is currently piloting the digital yuan and South Korea, the UK, Sweden, Thailand, and many other countries are also conducting research. A CBDC utilizes technology to represent a country's official currency in digital form. The Bahamas was the first country to launch a CBDC, called the sand dollar.

Unlike decentralized cryptocurrencies like Bitcoin, CBDCs are centralized and regulated by a country's monetary authority.

Important to the discussion about CBDCs is that there must be widespread adoption and liquidity in order for the abuse we are concerned about to happen. We are a long way from that point, but there are a number of potential concerns or risks that we could foresee if they were to be adopted on a larger scale. For example, if another country's CBDC were to instead be used to settle international trade transactions, that could increase the potential for sanctions evasion, and lessen the impact and effectiveness of U.S. sanctions. If financial transactions were conducted using CBDCs, rather than the U.S. dollar, which is the world's reserve currency, sanctions would likely become less impactful as transaction monitoring will bypass traditional screening processes currently used in financial messaging, such as SWIFT.

There are also a number of privacy concerns related to CBDCs. One potential national security concern is that other countries could gain insight into U.S. persons transacting with their CBDCs. For example, if U.S. persons downloaded the digital yuan app to send money to family in China, the Chinese government could potentially gain a great deal of information about them. This kind of cross border surveillance would be unprecedented. CBDCs could also make it easier for countries to gain strategic insight into US companies, which could provide companies in their country a competitive advantage. Countries could also more easily "cut off" companies that criticized them or that they did not want doing business in their country if they were using a CBDC controlled by that government than if they were using traditional payment systems.

3. ***Mr. Spiro and Mr. Lorber,*** *can you please discuss gap areas that are high risks for sanctions evasion but which are not covered by current law or regulation (or perhaps those in these areas believe that they have no obligations)? For example, there are Decentralized Finance platforms that are advertising their "No KYC" services, meaning that customers can avoid US and foreign anti-money laundering laws. There are also cryptocurrency tumbler and exchanger services designed to increase the anonymity of illicit transactions. We've seen these used by sanctions evaders and other bad actors.*
    a. *What is a viable response to close off or regulate these potentially dangerous avenues for those laundering ransoms, proliferation funds, and other dirty money?*

The cryptocurrency space is fast-evolving and the regulatory regime has not always maintained equal pace. Cryptocurrency exchanges are regulated as money services businesses, and required to register with the Financial Crimes Enforcement Network (FinCEN) and comply with Bank Secrecy Act requirements. The Department of Justice (DOJ) has leveraged this requirement to go after illicit cryptocurrency mixing and tumbling services. Recently, DOJ charged the operator of the "Helix" mixing service with "money laundering conspiracy, operating an unlicensed money transmitting business and conducting money transmission without a D.C. license."

However, there are other areas where regulations have not caught up with technology. As you point out, Decentralized Finance, or DeFi, platforms are not currently covered under our anti-money laundering and combating the financing of terrorism (AML/CFT) regime. Proper regulation of this

environment should focus on accountability and security in the DeFi ecosystem, without stifling the innovation happening in this burgeoning space.

One viable response is making these entities subject to the Bank Secrecy Act. This would ensure they meet certain AML/CFT requirements. Internationally, the Financial Action Task Force (FATF), the inter-governmental body that sets global standards relating to AML/CFT, is examining these gaps and looking at ways to mitigate them. They released updated draft guidance in March 2021 on how member jurisdictions should regulate and supervise the cryptocurrency ecosystem. Among the draft guidance were provisions that would designate DeFi protocols' "owners and operators" as VASPs, ensuring they fell under AML/CFT regulatory regimes. The finalized FATF guidance is expected to be released in October, at which point FATF members, including the United States, will implement the recommended policies through rulemaking or legislative processes.

4. ***All witnesses,*** *one of the most common evasion techniques is the use of front or shell companies.*
    a. *Can you comment on how sanctions targets use front companies and anonymous shell companies to evade sanctions, perhaps offering some illustrations of those cases?*

Chainalysis does not have any specific examples of the use of front companies or anonymous shell companies to access cryptocurrency exchanges to highlight. That said, enhanced due diligence is important in relation to the cryptocurrency ecosystem in order to ensure bad actors don't access cryptocurrency exchanges through front companies.

    b. Are there additional steps that Congress needs to complement the upcoming FinCEN registry on beneficial ownership?

A key element to ensuring the success of the FinCEN beneficial ownership registry will be ensuring that FinCEN has adequate resources. Currently, FinCEN has not been allocated sufficient resources to implement the Anti-Money Laundering Act, including the beneficial ownership registry. This should be a key focus for Congress.

5. *To what extent is cryptocurrency used to evade sanctions? (Asked live in hearing.)*

Just as with fiat currency, it is extremely difficult to estimate the extent of sanctions evasion with cryptocurrency. However, one benefit to cryptocurrency is the transparency that the blockchain provides and the educated estimates it allows us to make. Here Chainalysis attempts to expound upon the extent of sanctions evasion using cryptocurrency, noting caveats around the data where necessary. In some cases, we can calculate the amount flowing to cryptocurrency users in a country, but not necessarily the extent to which that amount represents sanctions evasion, for example. We elaborate on our estimates related to sanctions evasion using cryptocurrency and the limitations of the data in each section.

Digital Currency Addresses Included As Identifiers on the SDN List

Since November 2018, OFAC has included 97 digital currency addresses as identifiers in eight different designations on the Specially Designated Nationals and Blocked Persons List (SDN List), which financial

institutions screen their customers against. These are the most straightforward wallet addresses to examine, in terms of sanctions evasion. Using blockchain analysis, Chainalysis can see the effectiveness of including digital currency addresses as identifiers in designations. Our data demonstrates that after digital currency identifiers are included, little to no more cryptocurrency flows to these addresses, indicating the positive impact of blacklisting wallet addresses. The chart below demonstrates the total flow of cryptocurrency to digital currency addresses included as identifiers for sanctioned individuals and entities entries on the SDN List, and after their inclusion. As you can see, in total, these individuals received $167,141,613, but after their inclusion on the SDN list, the addresses received the USD equivalent of only $507.[2] In some cases, this may be because the malicious actors had ceased to use the addresses by the time of their inclusion, but in other instances, it demonstrates the effectiveness of cryptocurrency business' AML/CFT programs in stopping the flow of funds to sanctioned entities.

Chart Showing Impact of OFAC Including "Digital Currency Addresses" As Identifiers in Designations of Individuals and Entities[3]

Designating Body	Sanction Type	Sanctioned Individual or Entity	Total Received by Their Digital Currency Addresses Included as Identifiers on SDN List (in USD Value as of Date Received)	Sanction Date	Total Amount Received by These Addresses After Sanctions (in USD Value as of Date Received)
OFAC	SDN	ANDREYEV, Anton Nikolaeyvich	$950,504	9/10/2020	0
OFAC	SDN	GHORBANIYAN, Mohammad	$1,219,125	11/28/18	$1
OFAC	SDN	KARASAVIDI, Dmitrii	$45,908,480	9/16/20	$0.05
OFAC	SDN	KHORASHADIZADEH, Ali	$2,709,815	11/28/18	$6.84
OFAC	SDN	LI, Jiadong	$14,901,720	3/2/20	$1.14
OFAC	SDN	LIFSHITS, Artem Mikhaylovich	$4,179	9/10/20	$0
OFAC	SDN	RAZA, Mujtaba Ali	$5,544	4/20/2021	$0
OFAC	SDN	SECONDEYE	$2,599,328	4/15/2021	$487

[2] Funds sent to OFAC addresses after designation are often incredibly small amounts of cryptocurrency often referred to as "dust." Sending dust, or dusting, is a way to send messages, or advertise services, via vanity addresses or OP_Return messages on the blockchain. Dusting often happens with well-known and infamous addresses for advertising purposes.

[3] This chart is an updated version of the chart included in my written testimony, and includes updated data.

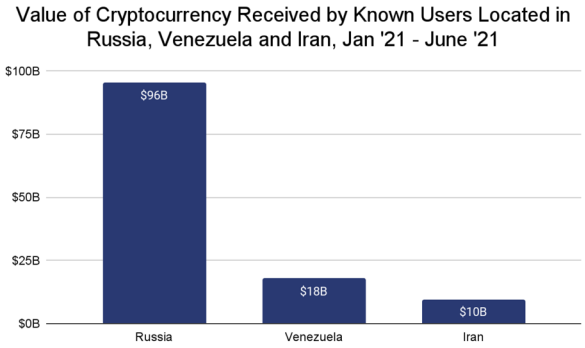
		SOLUTION			
OFAC	SDN	SOUTHFRONT	$11,886	4/15/2021	$10.75
OFAC	SDN	POTEKHIN, Danil	$8,732,388	9/16/2020	$0
OFAC	SDN	TIAN, Yinyin	$89,728,470	3/2/20	$0.15
OFAC	SDN	YAN, Xiaobing	$229,845	8/21/2019	$0.31
OFAC	SDN	ZHENG, Fujing	$76,827	8/21/2019	$0.05
OFAC	SDN	ZHENG, Guanghua	$63,503	8/21/19	$0.00
		TOTAL	**$167,141,613**		**$507**

Russia, Venezuela, and Iran

Using blockchain analysis data, Chainalysis can provide data about cryptocurrency flows in specific countries, including countries under comprehensive sanctions, or home to sanctioned individuals or entities. This is done by analyzing cryptocurrency flows through exchanges located in these jurisdictions or to users estimated to be located in these countries. Please see Appendix A for an explanation of the methodology used to determine where cryptocurrency users are located.

An important caveat with this data is that, depending on the jurisdiction, the sanctions regime there may not be comprehensive, so a portion -- perhaps even the majority -- of cryptocurrency flows to cryptocurrency users may be to legitimate users, rather than sanctioned entities or individuals. It is not possible to determine to whom specific wallet addresses belong to based on blockchain data, so further separation of the data is not possible. Therefore, this data represents *all* known transactions flowing to cryptocurrency users in these locations, rather than just those addresses associated with sanctioned entities or individuals. This data thus represents the *greatest* possible amount of sanctions evasion in these locations that we could identify. The true scope of sanctions evasion is likely much smaller than the numbers presented here.

Here we present the estimated value of cryptocurrency received by cryptocurrency users estimated to be located in Russia, Venezuela, and Iran. All three countries have robust cryptocurrency ecosystems, each generating a substantial amount of activity on the blockchain across all cryptocurrency assets. As noted above, this data represents an estimate of the overall flow of cryptocurrency to the cryptocurrency user base of people located in these countries, and *not* just to sanctioned individuals or entities.



As shown above, between January 2021 and June 2021, Russian cryptocurrency users received an estimated $96 billion in cryptocurrency. These cryptocurrency users very likely include many legitimate users of cryptocurrency, as well as some sanctioned entities. The United States does not maintain comprehensive sanctions against Russia, but rather maintains sanctions against Russian individuals, entities, and sectors for a number of different issues related to national security and human rights violations.[4] Perhaps most relevant to this discussion are sanctions that have been levied against Russian entities and associates for malicious cyber activities, including election interference-related activities. We know these entities use cryptocurrency, as digital currency addresses were included among their identifiers when they were added to OFAC's SDN List. Cryptocurrency belonging to these sanctioned entities are very likely captured among the $96 billion, but without their identified wallet addresses, we are unable to determine what portion of that overall number is associated with them.

Venezuelan cryptocurrency users received $18 billion in cryptocurrency between January 2021 and June 2021. As with the Russian example, these cryptocurrency users very likely include many legitimate users of cryptocurrency, as well as some sanctioned entities. The United States does not maintain comprehensive sanctions against Venezuela, but does block all property and interests in property of the Government of Venezuela and has levied additional drug and terror-related sanctions; sanctions related to anti-democratic actions, human rights violations, and corruption; as well as sectoral and financial sanctions.[5] In 2018, the Venezuelan government launched their own cryptocurrency, the Petro. While the goal of the Petro project was ostensibly to combat the currency devaluation hurting Venezuela today, government officials have also stated that evading sanctions is another goal.[6] It is therefore not

[4] U.S. Sanctions on Russia: An Overview. (2021, June 7). Congressional Research Service, IF10779 (Version 9). https://www.everycrsreport.com/files/2021-06-07_IF10779_06f76bfa979744a347c61e99204ce3a9e2c894cb.pdf

[5] Venezuela: Overview of U.S. Sanctions. (2021, January 22). Congressional Research Service, IF10715 (Version 35). https://crsreports.congress.gov/product/pdf/IF/IF10715

[6] Partz, H. (2020, September 30). Maduro claims crypto will play role in fighting sanctions against Venezuela. Cointelegraph. https://cointelegraph.com/news/maduro-claims-crypto-will-play-role-in-fighting-sanctions-against-venezuela

unreasonable to assume that some of the $18 billion in cryptocurrency flows to Venezuelan cryptocurrency users are tied to sanctions evasion.

Cryptocurrency users in Iran received $10 billion in cryptocurrency between January 2021 and June 2021. The United States has levied comprehensive sanctions against Iran, restricting imports, exports, and financial transactions with Iranians. However, as with Russia and Venezuela, these figures likely represent not only sanctions evasion, but legitimate use of cryptocurrency. There is a robust domestic Iranian cryptocurrency market, so many of these transactions could be Iranian-to-Iranian, and would therefore not represent sanctions evasion. It is unfortunately not possible to tell what percentage of the $10 billion is Iranian-to-Iranian transactions to give more clarity to this data.

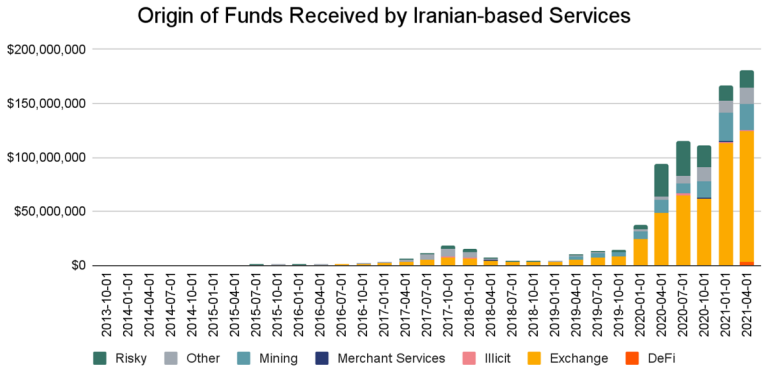
The two main ways Iran can use cryptocurrency to evade sanctions, or weaken the impact of sanctions, is to acquire wealth by mining or theft of cryptocurrencies, or to use cryptocurrencies to conduct economic business to bypass traditional screening. In addition to cryptocurrency sent to users based in Iran, Iran became heavily involved in mining cryptocurrencies in mid 2019. By mining cryptocurrencies, Iran is able to acquire wealth by validating cryptocurrency payments for individuals globally -- including U.S. citizens. They can then transact via non-traditional financial institutions, including high risk exchanges or individual peer-to-peer traders, to bypass screening. Iran's cyber actors have been involved with deploying ransomware and receiving cryptocurrency payments from U.S. companies.

While there has not been substantial reporting on exact use cases for economic trades involving cryptocurrency, Iran could use cryptocurrency to send and receive payments for oil or other goods to evade sanctions. According to a report from the English-language Iranian economic news source Financial Tribune, the Central Bank of Iran is authorizing banks and licensed exchanges to use cryptocurrency as payments for imports.[7]

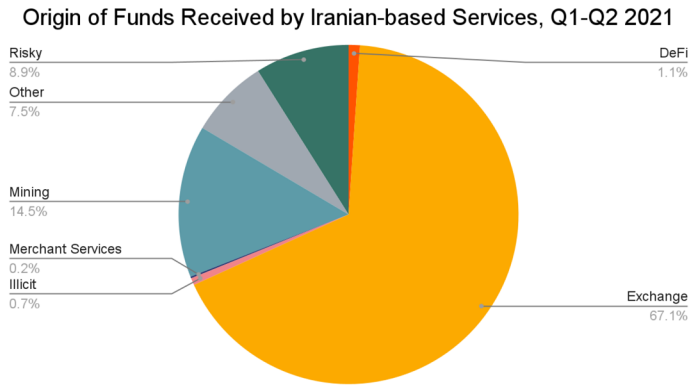
Below we outline the origin of funds received by Iranian-based services.[8] The predominant sender of funds to Iranian services are cryptocurrency exchanges, followed by mining pools.

[7] Financial Tribune. (2021, April 23). Banks and Forex Shops Can Use Digital Assets to Pay for Imports. https://financialtribune.com/articles/business-and-markets/108313/banks-and-forex-shops-can-use-digital-assets-to-pay-for-imports

[8] Categories: "Risky" contains gambling, mixing, high-risk exchanges, high-risk jurisdictions. "Illicit" contains darknet markets, fraud, scams, ransomware, stolen funds, child abuse material, terrorist financing, illicit actor organization, and sanctions. Please see Appendix B for further definitions.

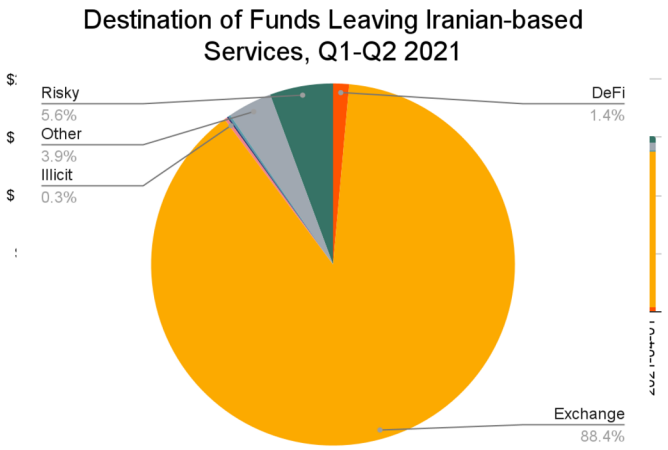


Here is the same data, presented in total as a pie chart rather than year on year.



Cryptocurrency exchanges are also the largest destination for funds leaving Iranian-based services, followed by risky services. Notably, most of the funds leaving Iranian services wind up on just one

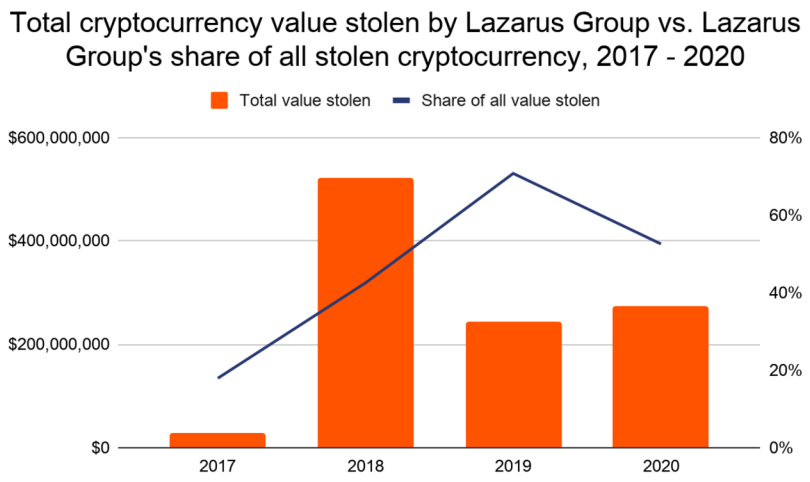
service. Many of these services, such as cryptocurrency exchanges, are plugged into global markets, which may present sanctions evasion opportunities.
Here is the same data, presented in total as a pie chart rather than year on year.



North Korea

The United States has levied comprehensive sanctions against North Korea, restricting imports, exports, and financial transactions with North Korea. They have also levied sanctions against North Korean malicious cyber actors. There are no known cryptocurrency services in North Korea, but North Korea is home to prolific hacking organizations generating billions of dollars in stolen cryptocurrency revenue. This includes the Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group. According to OFAC, "North Korea's malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges" and the stolen funds allow "the North Korean regime to continue to invest in its illicit ballistic missile and nuclear programs."[9] As cryptocurrency use has become more prominent, we have seen a corresponding increase in North Korean hacks of cryptocurrency exchanges, as depicted below. Overall, the group is believed to have stolen more than $1.75 billion worth of cryptocurrency in the time it's been active. The chart below outlines the total value stolen by Lazarus Group, as well as their share of all stolen cryptocurrency from 2017-2020.

[9] Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group. (2021, July 15). U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sm924



Currencies included: BAT, BCH, BNB, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Malicious Cyber Actors and Groups

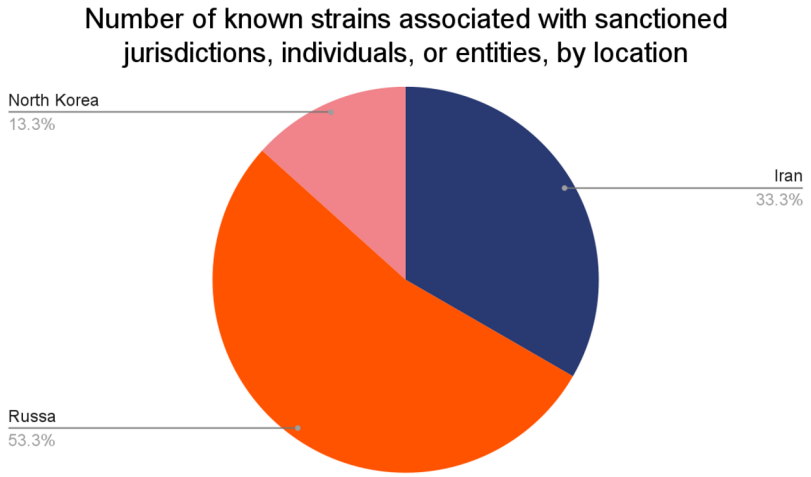
OFAC has also sanctioned malicious cyber groups. For example, OFAC sanctioned Evil Corp for its development and distribution of the Dridex malware strain, which was largely active in late 2015 and early 2016. Deployers of Dridex malware likely employed BitPaymer ransomware, according to CISC.[10] In response to such actions, Evil Corp adapted and moved to ransomware variants such as WastedLocker. Using blockchain analysis, it is possible to see this evolution happening -- one can identify Evil Corp actors and affiliates, as well as their facilitators. But if you rely only on the digital currency addresses included as identifiers in the Evil Corp sanctions listing, you may not realize this shift represented an attempt to evade sanctions.

Chainalysis has analyzed a number of different ransomware strains and identified those that pose a sanctions violation risk. In the chart below, we outline the different strains, why we believe they pose a sanctions violation risk, and the total amount of cryptocurrency they have received, in USD. In order to have been determined a sanctions violation risk, the strains had to meet one of three criteria: 1) Payments to addresses identified by OFAC as belonging to sanctioned individuals, 2) Payments to addresses Chainalysis has connected to ransomware strains whose creators have been sanctioned by OFAC, or 3) Payments to addresses connected to ransomware strains associated with cybercriminals

[10] Alert (AA19-339A): Dridex Malware. (Original release date: December 05, 2019 | Last revised: June 30, 2020) Cybersecurity and Infrastructure Security Agency CISA. us-cert.cisa.gov/ncas/alerts/aa19-339a

based in heavily sanctioned jurisdictions such as Iran and North Korea. It is important to note that these figures include payments made before sanctions were levied (if applicable), as well as after.

These numbers do not reflect sanctions evasion using cryptocurrency, but rather cryptocurrency use by groups under sanctions or affiliated with sanctioned entities.



Currencies included: BCH, BTC

Nearly all of the known ransomware payments with sanctions risk in 2020 and 2021 went to Doppelpaymer and WastedLocker. In previous years, Bitpaymer, SamSam, and Locky have also been responsible for a high volume of ransomware payments associated with sanctions risk. So far in 2021, Phoenix CryptoLocker has been responsible for the vast majority of ransomware payments associated with sanctions risk. We should also note that there are reports of increased activity from Iranian ransomware strains with sanctions risk in 2021, though our data doesn't yet confirm this trend.

Dealing with a ransomware attack is incredibly stressful. In cases where hospitals and other critical infrastructure systems have been attacked, lives have been at risk where computer systems were rendered inoperable. It is imperative that businesses and government entities prepare in advance so that during a stressful situation, a plan is already in place. Having a ransomware response plan that includes working with subject matter experts, who can coordinate with law enforcement and perform the necessary blockchain analytics on proposed payments to avoid sanctions violations, is critical.

Terrorist Groups

Chainalysis has identified cryptocurrency wallet addresses tied to a number of designated terrorist groups and affiliates. Not all of this cryptocurrency use can be categorized as sanctions evasion, though. Below we look at just those groups that have been designated as terrorist organizations -- or tied directly to designated terrorist organizations -- and included on OFAC's SDN list and the amount of money the wallet addresses known to belong to those groups have received.

Terrorist Group	Related Sanctions	Amount Received in Cryptocurrency (USD Value at the time received)
Hamas	Hamas is a designated FTO and included in OFAC's SDN list	$500,251
Hamas Al-Qassam Brigades	Al-Qassam Brigades, is the military arm of Hamas, which is a designated FTO and included in OFAC's SDN list.	$138,914
Ibn Taymiyya Media Center	Ibn Taymiyya Media Center (ITMC) is the media wing of Mujahideen Shura Council in the Environs of Jerusalem, a jihadist group based in Gaza that is a designated FTO and included in OFAC's SDN list.	$16,088
Katibat Tawhid wal Jihad	Katibat Tawhid wal Jihad is a primarily Uzbek jihadi battalion operating in the northwest of Syria. Pledged their allegiance to Al Qaeda in Syria (Jabhat Al-Nusrah), which is a designated FTO and included in OFAC's SDN list.	$15,807
Malhama Tactical	Malhama Tactical is an Uzbek jihadi group affiliated with Jabhat Fateh Al-Sham, which is a designated FTO and included in OFAC's SDN list.	$1,194

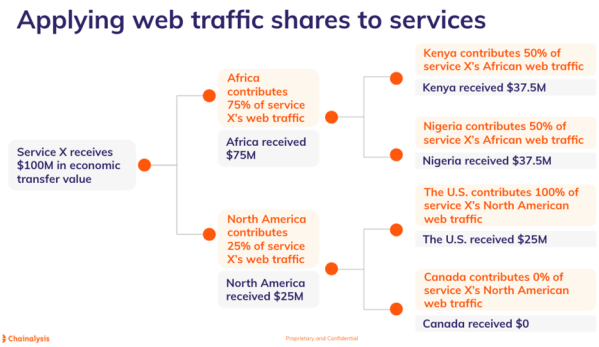
APPENDIX A

Please note that due to the decentralized nature of cryptocurrency, it is difficult, if not impossible to know the true amount of cryptocurrency usage in a country.

How Chainalysis' calculates the geography estimates

Country-level estimates are based on service-level activity, multiplied by the web traffic share of countries' users visiting the site on a monthly time-series. All activity belonging to a country is then summed.

Example:



Additional factors considered when assigning activity to a country/region:

- Time zone analysis of platforms' cryptocurrency activity, fiat currency pairs offered by the exchange, website language options, location of headquarters.

Caveats to our approach

1. Limitations of on-chain data: not all activity of interest occurs on the blockchain
    - Chainalysisdoes not capture cryptocurrency trading volume when someone purchases crypto with fiat and keeps it on an exchange, trades on an exchange, or cashes out on an exchange. This activity is not recorded on the blockchain, but rather is recorded in exchanges' private order books.
    - Chainalysis does have a subset of order book data from two popular P2P exchanges (LocalBitcoins and Paxful) but do not account for other off-chain data

2. Limitations of web traffic methodology: Chainalysis uses a service's web traffic shares to estimate cryptocurrency usage
    - The relationship between web searches and cryptocurrency activity is not 1-to-1 (it's the best estimate, but is an estimate)
    - The web traffic data does not account for VPN usage: at times we pick up a different country than where a person actually is
    - Bias by transfer size: Chainalysis applies web traffic shares regardless of transfer size, likely underestimating users in a country making large transfers
    - While Chainalysis' website domain data is robust, there may be cryptocurrency domains Chainalysis is unaware of that would not be captured within these estimates.

APPENDIX B

Category Definitions

Child abuse material site
Child abuse material includes forums and sites operating on the dark web which facilitate the buying, selling, and the spread of child sexual abuse material. These sites are often coded and difficult to access.

Darknet markets
Darknet markets are commercial websites that operate on the dark web, which can be accessed via anonymizing browsers or software such as Tor or I2P. These sites function as black markets by selling or advertising illicit goods and services such as drugs, fraud materials, and weapons, among others. Darknet markets use cryptocurrency payment systems, often with escrow services and feedback

systems to help develop trust between the vendor and customer. Darknet markets have become more security conscious over the past few years due to multiple law enforcement shutdowns.

DeFi
"DeFi" stands for "decentralized finance". It refers to the ecosystem of protocols and platforms that provide fully automated financial services built on top of smart contract-enriched blockchains — primarily the Ethereum network. DeFi protocols fulfil specific financial functions in accordance with predefined rules, as specified by the underlying smart contract code. This means they can execute transactions — trades, loans, etc. — automatically when specific conditions are met. The blockchain technology removes the need for a centralized third-party to mitigate counterparty risk or human intervention to keep it going, reducing fees. The non-custodial nature of DeFi also means users and investors remain in control of their funds. As DeFi is usually permissionless, a wider range of services and markets can be served compared to other fintech applications or financial institutions. DeFi protocols are interoperable and can be connected up and built on top of, often termed 'money legos'.

Exchanges
Exchanges allow users to buy, sell, and trade cryptocurrency. They represent the most important and widely-used service category in the cryptocurrency industry, accounting for 90% of all funds sent by services.

Fraud shop
Financially motivated shops selling different types of data including, PII (Personally Identifiable Information), credit card data, stolen accounts, and more. Unlike Darknet Markets, Fraud Shops are normally operated by a single actor/team and are the sole merchant within the service. Fraud shops also tend to have behavioral differences from darknet markets such as top-up depositing of funds (incremental increases to the total amount), as well as no customer withdrawals. Therefore, most outgoing transactions can be linked to the operators of the Fraud Shop.

Gambling
Online gambling can take many forms from resembling a typical casino where you can play card games like blackjack and poker, slot games and the like, to sites for wagering bets on sports or eSports outcomes.

The industry has been an early adopter of cryptocurrency. Users will send cryptocurrency as a convenient alternative to fiat, and get started betting. Gambling is treated differently depending on the jurisdiction, and many sites have lax KYC requirements. Because of this, there's potential for these sites to be used for laundering money. Many of these companies are located in/operating out of island nation-states (such as Curaçao, Cyprus, or Malta).

High risk exchange
Chainalysis' designates an exchange as high risk according to the following criteria:

- **No KYC**: The exchange requires no customer information before allowing any level of deposit or withdrawal. This is also applicable if they require name, phone number, or email address but do not attempt to verify that this information actually belongs to the customer.
- **Criminal ties**: The exchange has publicly documented ties to criminal activity.

- **High risky exposure**: The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing. Chainalysis examines if the exchange's exposure to illicit activity is an outlier compared to other exchanges. A service with direct high risk exposure one standard deviation away from the average across all exchanges identified by Chainalysis over a 12 month period is considered a high risk exchange.

High risk jurisdiction
The high risk jurisdiction category comprises cryptocurrency services that are based in specific jurisdictions, including Iran and Venezuela. Chainalysis considers both cryptocurrency activity as well as the global regulatory landscape when deciding which jurisdictions to include in this category. Given stringent guidelines for the financial system's interactions with Iran and Venezuela, Chainalysis has opted to more prominently surface services operating in these areas. Chainalysis will continue to add services to this category over time.

Illicit actor organization
Individuals and/or organizations that operate directly or indirectly in various forms of illicit activities. These entities are directly or indirectly involved with risky entities such as darknet markets, fraud shops, extremist financing, hacking, etc.

Merchant services
Merchant services are authorized financial services that enable businesses to accept payments on their customer's behalf. They are also known as payment gateways or payment processors. These services allow merchants to accept cryptocurrency for invoicing and online or in-person payments. This often includes conversion to local fiat currency and settling funds to the merchant's bank account.

Merchant services is generally a low-risk category. Users mostly comprise mainstream, traditional businesses on one end and their customers on another. However, it's worth noting that scammers sometimes integrate merchant services with a malicious website to accept cryptocurrency payments from their victims.

Mining and Mining pools
Mining is the process by which cryptocurrency is generated. Mining pools are special services where miners can pool their resources - typically GPU or specialized ASIC mining hardware - together towards mining cryptocurrency. By pooling mining resources the pool has a bigger chance of mining a block and the returns are divided among all the miners according to how much mining power each contributed.

Mining pools typically only receive funds from direct mining activity, and as such are typically low risk. However, a pool that accepts deposits from sources other than mining can be exploited for money laundering.

Mining is used for coin generation, when new coins are minted from the mining process.

Mixing services

Mixers are websites or software used to create a disconnection between a user's deposit and withdrawal. Mixing is done either as a general privacy measure or for covering up the movement of funds obtained from theft, darknet markets, or other illicit sources.

Mixers typically pool incoming funds from many users and re-distribute those funds with no direct connection back to the original source.

Other
This category is used when the entity does not represent a widely popular field of operation or is a particular type of operation or entity such as donation addresses, social network bots, seized funds, among others. This category does not have any inherent risk but may contain risky entities.

Ransomware
Ransomware is special malware designed to encrypt a victim's computer data and automatically request a ransom to be paid in order to decrypt the data. Attackers employ social engineering and phishing schemes that trick people and organizations into downloading the malicious software.

Sanctions
Sanctions refer to entities listed on economic/trade embargo lists, such as by the US, EU, or UN, with which anyone subject to those jurisdictions is prohibited from dealing. Currently this includes the Specially Designated Nationals (SDN) list of the US Department of the Treasury's Office of Foreign Assets Control (OFAC). The prohibition on dealing includes any instrumentalities of the sanctioned entities, including operating companies, bank accounts, and cryptocurrency addresses used by the sanctioned entities. In some instances, persons subject to those jurisdictions are also required to block/freeze assets belonging to the sanctioned entities to prevent further benefit or movement.

Scam
Scams can impersonate a variety of services, including exchanges, mixers, ICOs, and gambling sites. This category also encompasses scam emails, extortion emails, and fake investment services. They usually offer unrealistic returns on investment, many times trying to mask a pyramid scheme, or pretend to have incriminating personal data on the victim and ask for money in order to not disclose it.

Stolen funds
Stolen funds comprise instances of hacked exchanges and services. Attackers engage in sophisticated and persistent social engineering, and exploit pre-existing vulnerabilities to transfer funds from exchange hot wallets to their control. The payoff for actors can be enormous with single incidents often resulting in tens of millions of dollars in losses.

Terrorist financing
Terrorist financing pertains to the funding of designated terrorist groups and affiliates of terrorist groups, entities, and individuals. Financing is fundamental for the survival and operation of terrorist groups and is used to support a multitude of their activities, including recruitment, propaganda, day-to-day activities, and military operations. Terrorist groups secure the flow of funds in a variety of ways, including through the use of cryptocurrencies.


DIRTY MONEY POURS INTO
THE WORLD'S MOST POWERFUL
BANKS.

THE FINCEN FILES

Thousands of secret suspicious activity reports offer a never-before-seen picture of corruption and complicity —

and how the government lets it flourish.

By Jason Leopold, Anthony Cormier, John Templon, Tom Warren, Jeremy Singer-Vine, Scott Pham, Richard Holmes, Azeen Ghorayshi, Michael Sallah, Tanya Kozyreva, and Emma Loop

Alex Fradkin / Redux for BuzzFeed News; BuzzFeed News; Getty Images; Alamy

Posted on September 20, 2020, at 1:01 p.m. ET

This is part of the FinCEN Files investigation. To read more, click here. Want to help us expose corruption and hold the highest levels of power to account? Become a BuzzFeed News Member here.

A huge trove of secret government documents reveals for the first time how the giants of Western banking move trillions of dollars in suspicious transactions, enriching themselves and their shareholders while facilitating the work of terrorists, kleptocrats, and drug kingpins.

And the US government, despite its vast powers, fails to stop it.

Today, the FinCEN Files — thousands of "suspicious activity reports" and other US government documents — offer an unprecedented view of global financial corruption, the banks enabling it, and the government agencies that watch as it flourishes. BuzzFeed News has shared these reports with the International Consortium of Investigative Journalists and more than 100 news organizations in 88 countries.

These documents, compiled by banks, shared with the government, but kept from public view, expose the hollowness of banking safeguards, and the ease with which criminals have exploited them.

Profits from deadly drug wars, fortunes embezzled from developing countries, and hard-earned savings stolen in a Ponzi scheme were all allowed to flow into and out of these financial institutions, despite warnings from the banks' own employees.

Money laundering is a crime that makes other crimes possible. It can accelerate economic inequality, drain public funds, undermine democracy, and destabilize nations — and the banks play a key role. "Some of these people in those crisp white shirts in their sharp suits are feeding off the tragedy of people dying all over the world," said Martin Woods, a former suspicious transactions investigator for Wachovia.

"Some of these people in those crisp white shirts in their sharp suits are feeding off the tragedy of people dying all over the world."

Laws that were meant to stop financial crime have instead allowed it to flourish. So long as a bank files a notice that it may be facilitating criminal activity, it all but immunizes itself and its executives from criminal prosecution. The suspicious activity alert effectively gives them a free pass to keep moving the money and collecting the fees.

The Financial Crimes Enforcement Network, or FinCEN, is the agency within the Treasury Department charged with combating money laundering, terrorist financing, and other financial crimes. It collects millions of these suspicious activity reports, known as SARs. It makes them available to US law enforcement agencies and other nations' financial intelligence operations. It even compiles a report called "Kleptocracy Weekly" that summarizes the dealings of foreign leaders such as Russian President Vladimir Putin.

What it does not do is force the banks to shut the money laundering down.

In the rare instances when the US government does crack down on banks, it often relies on sweetheart deals called deferred prosecution agreements, which include fines but no high-level arrests. The Trump administration has made it even harder to hold executives personally accountable, under guidance by former deputy attorney general Rod Rosenstein that warned government agencies against "piling on." Rosenstein did not respond to requests for comment, but after this article was published, he wrote to say that his policies sought to "encourage prosecutors to pursue charges against the people responsible for corporate wrongdoing."

The FinCEN Files investigation shows that even after they were prosecuted or fined for financial misconduct, banks such as JPMorgan Chase, HSBC, Standard Chartered, Deutsche Bank, and Bank of New York Mellon continued to move money for suspected criminals.

Suspicious payments flow around the world and into countless industries, from international sports to Hollywood entertainment to luxury real estate to Nobu sushi restaurants. They filter into the companies that make familiar items from people's lives, from the gas in their car to the granola in their cereal bowl.

The FinCEN Files expose an underlying truth of the modern era: The networks through which dirty money traverse the world have become vital arteries of the global economy. They enable a shadow financial system so wide-ranging and so unchecked that it has become inextricable from the so-called legitimate economy. Banks with household names have helped to make it so.

The Bank of America tower in New York City.

Deutsche Bank's US headquarters in New York City.

The Standard Chartered headquarters in London.

A JPMorgan Chase location in New York City.

Alex Fradkin / Redux for BuzzFeed News

BuzzFeed News' investigation shows that:

BuzzFeed News **Deadly Terror Networks And Drug Cartels Use Huge Banks**

- Standard Chartered moved money on behalf of Al Zarooni Exchange, a Dubai-based business that was later accused of laundering cash on behalf of the Taliban. During the years that Al Zarooni was a Standard Chartered customer, Taliban militants staged violent attacks that killed civilians and soldiers.

- HSBC's Hong Kong branch allowed WCM777, a Ponzi scheme, to move more than $15 million even as the business was being barred from operating in three states. Authorities say the scam stole at least $80 million from investors, mainly Latino and Asian immigrants, and the company's owner used the looted funds to buy two golf courses, a 7,000-square-foot mansion, a 39.8-carat diamond, and mining rights in Sierra Leone.

- Bank of America, Citibank, JPMorgan Chase, American Express, and others collectively processed millions of dollars in transactions for the family of Viktor Khrapunov, the former mayor of Kazakhstan's most populous city, even after Interpol issued a Red Notice for his arrest. Khrapunov, who had already fled to Switzerland and who claims the allegations are politically motivated, was later convicted in absentia on charges that included bribe-taking and defrauding the city through the sale of public property.

The banks mentioned in this story said they could not comment on specific transactions due to bank secrecy laws. Their statements can be found here.

By law, banks must file suspicious activity reports when they spot transactions that bear the hallmarks of money laundering or other financial misconduct, such as large, round-number transactions or payments between companies with no discernible business relationship. SARs are not by themselves evidence of a crime, but FinCEN's director, Kenneth Blanco, has called them "vital for law enforcement investigations."

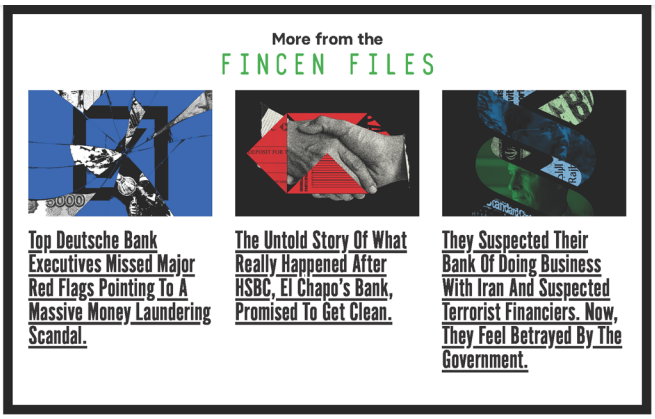
Prior to this reporting, very few SARs had ever been revealed. The FinCEN Files encompass more than 2,100.

Information from millions of these documents feeds into a single database, through which law enforcement officers can summon detailed financial information with a few keystrokes. The FinCEN Files opens a rare window into this vast system of financial intelligence, unmatched in the world but all but unknown to the public. The SARs themselves are so closely held that members of the public cannot obtain them through records requests or subpoenas, and banks are not allowed even to confirm their existence.

Prior to this reporting, very few SARs had ever been revealed. The FinCEN Files encompass more than 2,100.

For more than a year, BuzzFeed News and its partner news organizations across the world mined the information on these tens of thousands of pages to map more than 200,000 transactions. (Here's an explanation of how we did it.) In all, suspicious activity reports in the FinCEN Files flagged more than $2 trillion in transactions between 1999 and 2017. Western banks could have blocked almost any of them, but in most cases they kept the money moving and kept collecting their fees.

Suspicious activity reports are written by the banks' financial crime watchdogs, or compliance officers, who are often parked in remote offices and left to make sense of a vast number of transactions with very few resources, writing SARs with little research or verification. BuzzFeed News' research went much further, including reams of internal bank data, thousands of pages of public records, hundreds of interviews with sources across the globe, dozens of Freedom of Information Act filings, five public records lawsuits, and requests for three federal courts to unseal records — all to piece together the intricacies of a financial system that is largely hidden.



BuzzFeed News is not publishing the SARs in full because they contain information about people or companies that are not under suspicion, but who were swept up in the banks' searches. A subset of the documents is being published, with redactions, to support reporting in specific stories.

After the Treasury Department received detailed questions about the FinCEN Files investigation, the agency released a statement saying that it was "aware that various media outlets intend to publish a series of articles based on unlawfully disclosed Suspicious Activity Reports (SARs)." It continued, "the unauthorized disclosure of SARs is a crime that can impact the national security of the United States, compromise law enforcement investigations, and threaten the safety and security of the institutions and individuals who file such reports." The agency announced that it was referring the matter to the Department of Justice and the Treasury Department's Office of Inspector General.

In a subsequent letter, FinCEN's general counsel said that disclosure of SARs can make banks less willing to file them, which "could mean law enforcement has fewer potential leads to stop crimes like human

trafficking, child exploitation, fraud, corruption, terrorism, and cyber-enabled crime."

FinCEN did not respond to repeated invitations to discuss security concerns.

Sen. Ron Wyden, a member of the Senate Intelligence Committee, which requested some of these SARs, said the FinCEN Files investigation "reinforces the fact that we now have two systems of law enforcement and justice in the country." Drug cartels move millions through US banks; poor people go to jail for possession. "If you're wealthy and well-connected, you can figure out how to do an enormous amount of harm to society at large and ensure that it accrues to enormous financial benefit for all of you."

Robert Mazur, a former federal special agent and an expert in money laundering, said that making this material public "could enhance national security, aid future investigations, and encourage institutions to more consistently adhere to SAR filing requirements," and "will hopefully get people who are in a position of power to correct an apparent systemic failure."

A Historic Opportunity

ge Banks

The United States Treasury Department in Washington, DC
Alex Fradkin / Redux for BuzzFeed News

Based in the United Arab Emirates, Mazaka General Trading presented itself to the world as a wholesaler.

But between March 2013 and April 2014, the company received nearly $50 million from five companies involved in a Russian money laundering ring that manipulated international stock trades. In May and June 2014, it received more than $4 million from a Singapore company that appears barely even to exist. It was also sending and receiving money from British firms located at 175 Darkes Lane, one of the world's most notorious addresses for shell companies, which are a common tool to hide ownership.

These transactions by Mazaka General Trading — which the Treasury Department later declared to be a part of the Khanani money laundering network, a group that has financed terrorism and drug cartels around the globe — involved businesses and people far from the shores of the United States. But as the money pinged around from one bank to another, it was all being tracked and it would all be reported to the Treasury Department.

Because the US dollar is the lifeblood of international finance, the common denominator between the world's disparate currencies, banking customers around the world need access to it. But only select banks are licensed to conduct dollar transactions. So smaller banks in other countries partner with larger institutions, which exchange their customers' pesos, yuan, or dirham for greenbacks. For a fee, the

arrangement, known as correspondent banking, helps keep the global economy humming.

As they pass through US banks, these transfers give the Treasury Department a vantage that no other country has.

It shares some of that information through the Egmont Group, a little-known coalition of financial intelligence units from more than 150 countries and territories. SARs have provided Egmont members with financial details that would be otherwise unattainable, such as those concerning former Olympic Committee member Lamine Diack, who has been sentenced to prison for crimes connected to the Russian doping scandal, and the Russian oligarch Oleg Deripaska, who was sanctioned by the US two years ago. (Deripaska has sued the US government, maintaining that he is an innocent victim of politics.)

But if the database is a powerful asset to law enforcement investigations, to privacy advocates, it is a nightmare of overreach.

Congress created the current SAR program in 1992 making banks the frontline in the fight against money laundering. But Michael German, a former FBI special agent who is a national security and privacy expert, said that after 9/11, "the SAR program became more about mass surveillance than identifying discrete transactions to disrupt money launderers."

Today, he said, "the data is used like the data from other mass surveillance programs. Find someone you want to get for whatever reason then sift through the vast troves of data collected to find anything you can hang them with."

In 2017, when US congressional committees began investigating the last presidential election and other matters, they, too, turned to the Treasury Department database.

They requested SARs on Deutsche Bank, which had loaned Trump money; Christopher Steele, the former MI6 agent who wrote the so-called Trump dossier; an array of Russian oligarchs; Trump's former campaign chairperson Paul Manafort; and even a small casino in the Pacific run by a former Trump employee. All told, they were looking for information on more than 200 entities.

The world's biggest banks did business with clients they suspected were corrupt.

FinCEN unearthed tens of thousands of pages of documents. Those documents, along with a few additional SARs requested by federal law enforcement authorities, make up the majority of the FinCEN Files. Some were never turned over to the committees that requested them. A person familiar with the matter blew the whistle to multiple members of Congress.

The collection does not include any SARs about Trump's finances. (A source familiar with the matter told BuzzFeed News that FinCEN's database did not contain SARs on either Trump or the Trump Organization.) And though the documents show suspicious payments to people in Trump's orbit before and after key moments in the 2016 presidential campaign, they do not provide direct information on any election interference.

Because the searches were so broad, however, they revealed something that most in Congress hadn't even been looking for: evidence that the world's biggest banks kept doing business with clients that they themselves suspected were facilitating terror and corruption.

The information was laid out in transaction by transaction. And it had been there all along.

The FinCEN headquarters in Vienna, Virginia
Alex Fradkin / Redux for BuzzFeed News

FinCEN received more than 2 million SARs last year. That number has nearly doubled over the past decade, as financial institutions have faced mounting pressure to file and the volume of international transactions has grown. Over the same period, FinCEN's staff has shrunk by more than 10%. Sources there say most SARs are never even read, let alone acted upon.

Meanwhile, experts say, some banks treat SARs as a kind of get-out-of-jail-free card, filing alerts about a huge array of transactions without actually moving to halt them. In some cases, banks filed numerous reports on the same clients, detailing their suspected crimes over the course of years while continuing to welcome their business.

By December 2013, JPMorgan Chase had filed at least eight SARs on [illegible] transactions controlled by Mahmoud Hajjar, tagging more than

$10 million, according to a FinCEN research report. Manafort, who went on to become Trump's campaign chair, was convicted of bank and tax fraud in 2018.

Some banks treat SARs as a kind of get-out-of-jail-free card, filing alerts about a huge array of transactions without actually moving to halt them.

Paul Pelletier, a former senior Justice Department lawyer who once led the agency's fraud unit, said that approach makes a mockery of the system. "You can't just file SAR after SAR after SAR without eventually violating the money laundering laws," he said. "You cut them off and drop them as clients. But you don't keep taking their money."

Despite the banks' sweeping powers to investigate account holders, the FinCEN Files investigation reveals that major financial institutions often fail to perform the most basic checks on their customers, such as verifying where a business is located when someone opens a new account. The lapses allow criminal groups to hide behind shell corporations, registered with no identifying details about their ownership, and slide the proceeds of their crimes into the global financial system.

In many cases, the banks appear to have no idea whatsoever whose money they are moving.

When investigators for HSBC's American operations asked their colleagues in Hong Kong for the name of the person who owned Trade Leader, a company that had moved more than half a billion dollars through the bank in less than two years, the answer they got was "None available." The company would reportedly emerge as an important hub in the so-called Russian Laundromat, a sprawling scheme in which wealthy Russians, facilitated by banks, secretly moved their money into the West.

After scandals like the Russian Laundromat, federal prosecutors have made big pronouncements about forcing meaningful change.

Addressing an anti–money laundering conference in 2015, Leslie Caldwell, then the head of the Justice Department's criminal division, said that when it came to getting banks to clean up their acts, deferred prosecution agreements, which typically involve a fine and a probationary period, "can often accomplish as much as, and sometimes even more than, we could from a criminal conviction."

But the FinCEN Files investigation shows something very different. Banks often get to the end of their agreement without actually fixing the problems. Then, instead of getting the prosecution that they had been threatened with, they just get another chance. And sometimes another.

In 2012, HSBC faced a historic crisis. After permitting narcotraffickers to launder money and conducting business in off-limits countries such as Sudan and Myanmar, the bank was fined $1.9 billion. It promised to change its ways, and to hold it to that promise, the government installed an independent monitor to keep close watch. But the FinCEN Files investigation shows HSBC continued banking, and profiting from, the same kinds of customers that got it in trouble in the first place, such as a Panamanian import-export firm that the Treasury Department later said was laundering money for drug kingpins.

JPMorgan Chase got a deferred prosecution deal of its own. For years, it was the primary bank of the world's biggest Ponzi schemer, Bernie Madoff. Despite multiple warnings from its own employees, the bank never filed a suspicious activity report on him and allegedly collected $500 million in fees. For punishment, the bank was required to pay a $1.7 billion fine and promise to improve its money laundering defenses. But after it settled the Madoff case, the bank's own [illegible] suspected fraud reports to accounts of an

alleged Russian organized crime figure who is known for drug trafficking and contract murders, as well as businesses tied to the repressive North Korean regime, which the US has placed off-limits.

It happened at Standard Chartered, too. Last year, the government amended its 2012 deferred prosecution agreement after the bank was found to have continued clearing transactions for individuals and businesses in off-limits countries, primarily Iran. The bank paid fines totaling $1.1 billion to US and UK authorities, and extended the terms of the deferred prosecution agreement for the sixth time in the space of seven years. The bank apologized for its "violations and control deficiencies" but promised that none had occurred after 2014.

The FinCEN Files documents show Standard Chartered processed hundreds of millions of dollars for companies it suspected were circumventing sanctions against Iran until at least 2017.

Since 2010, at least 18 financial institutions have received deferred prosecution agreements for anti–money laundering or sanctions violations, according to an analysis by BuzzFeed News. Of those, at least four went on to break the law again and get fined. Twice, the government responded to this kind of repeat offense by renewing the deferred prosecution agreement — the very tool that failed the first time.

Can It Be Fixed?

ge Banks

The Bank of America Tower in New York City
Alex Fradkin / Redux for BuzzFeed News

If the government wanted to, experts in financial crime say, it could stop the dirty money coursing through the big banks, as well as the vast array of criminal activity it funds.

One step would be to require companies to disclose their owners to the Treasury Department, rather than allowing people to hide behind a shell company. Lawmakers are debating a bipartisan bill that could address that for small companies. The National Federation of Independent Business has opposed it, saying it raises privacy issues and would increase costs. Sen. Sherrod Brown, who cosponsored the bill, told BuzzFeed News, "Congress must act soon because criminals have long been revising, adjusting, and amending their tactics to circumvent our laws."

Greater public accountability could also make a difference. HSBC has fought to keep secret the final report by the monitor that the government installed to watch over the bank during the years of its deferred prosecution agreement. It even took the unusual step of weighing in on a Freedom of Information Act lawsuit, when BuzzFeed News sued the Justice Department to release the report. The knowledge that negative reports could become public, and potentially damage share prices, could impel wayward banks to clean up their

“The bankers will never learn until you start putting silver bracelets on people.”

Others say the SARs themselves are part of the problem. German, the former FBI special agent, called the idea behind them "naive" because "the largest money laundering operations occur with the cooperation of the financial institutions, or at least some officers within those institutions. The lack of money laundering enforcement had nothing to do with a lack of evidence of suspicious transactions, but a lack of interest by political and law enforcement leadership.”

The most powerful way to fix the problem might be the simplest: Arrest the executives whose banks break the law. "The bankers will never learn until you start putting silver bracelets on people," Pelletier said. "Think of the message you're sending to repeat offenders."

"These guys know what they're doing,” said Thomas Nollner, a former regulator with the Office of the Comptroller of the Currency. “You break the law, you should go to jail, period."

That approach was once the norm. “Back in the 1980s and 90s and even into the early 2000s, the government went after CEOs all the time,” said US District Judge Jed Rakoff, who has been an outspoken critic of weak penalties for white-collar criminals. In the past, the CEOs of Enron, WorldCom, and Tyco were all sent to jail for what they did, he pointed out. “Now that’s deterrence.”

Rakoff went further: “Under US law, a bank that engages in money laundering can literally be forced out of business by the government, and it is kind of surprising that government hasn’t taken that step, given the obvious deterrent effect it would have.”

Ultimately, the power to keep criminal profits from being laundered through the US financial system may not reside in the actions of a

tier. It may not reside with banking regulators or federal prosecutors or FinCEN. It may not even be a matter of national policy alone. Shutting down wayward banks could have an impact on the whole economy — for the US, its major trade partners, and beyond. When other countries find their banks under US scrutiny, they step in.

In 2012, Standard Chartered and HSBC were facing criminal prosecution. George Osborne, at that time the UK's chancellor of the exchequer, wrote to the chairperson of the US Federal Reserve, Ben Bernanke, and Treasury Secretary Timothy Geithner to discuss his "concerns" that a heavy-handed response could have "unintended consequences." He warned of a "contagion." The implication: Close one bank and the whole economy could suffer.

Prosecutors stood down.

Mazur, the former federal special agent and money laundering expert, says there are a "mosaic" of reasons why US authorities let the money keep running, but one of them may just be that it finds its way into too many pockets.

"Even if it's bad wealth, it buys buildings," he said. "It puts money into bank accounts. It enriches the nation." ●

Sophie Comeau, Waylon Cunningham, Sam Feehan, Nancy Guan, Kristy Hutchings, Kylie Storm, Felicia Tapia, Karen Wang, Abby Washer, and Ashley Zhang of the USC Annenberg School for Communication and Journalism contributed reporting.

This article has been updated with a comment by former deputy attorney general Rod Rosenstein.

Jason Leopold is a senior investigative reporter for BuzzFeed News and is based in Los Angeles. He is a 2018 Pulitzer finalist for international reporting, recipient of the IRE 2016 FOI award and a 2016 Newseum Institute National Freedom of Information Hall of Fame inductee.

Contact Jason Leopold at jason.leopold@buzzfeed.com.

Got a confidential tip? Submit it here.

Anthony Cormier is an investigative reporter for BuzzFeed News and is based in New York. While working for the Tampa Bay Times, Cormier won the 2016 Pulitzer Prize for Investigative Reporting.

Contact Anthony Cormier at anthony.cormier@buzzfeed.com.

John Templon is a data reporter for BuzzFeed News and is based in New York. His secure PGP fingerprint is 2FF6 89D6 9606 812D 5663 C7CE 2DFF BE75 55E5 DF99

Contact John Templon at john.templon@buzzfeed.com.

Tom Warren is an investigations correspondent for BuzzFeed News and is based in London.

Contact Tom Warren at tom.warren@buzzfeed.com.

Jeremy Singer-Vine is the data editor for the BuzzFeed News investigative unit and is based in New York.

Contact Jeremy Singer-Vine at jeremy.singer-vine@buzzfeed.com.

Scott Pham is a data reporter for BuzzFeed News and is based in New York.

Contact Scott Pham at scott.pham@buzzfeed.com.

Richard Holmes is an investigations reporter for BuzzFeed News and is based in London.

Contact Richard Holmes at richard.holmes@buzzfeed.com.

Michael Sallah was an investigative reporter for BuzzFeed News and is based in Washington, DC.

Contact Michael Sallah at michael.sallah@buzzfeed.com.

Tanya Kozyreva was an investigative correspondent for BuzzFeed News based in Kiev, Ukraine.

Contact Tanya Kozyreva at tanya.kozyreva@buzzfeed.com.

Emma Loop was a political reporter for BuzzFeed News and is based in Washington, DC.

Contact Emma Loop at emma.loop@buzzfeed.com.

Azeen Ghorayshi is a science editor for BuzzFeed News and is based in New York.

Contact Azeen Ghorayshi at azeen.ghorayshi@buzzfeed.com.

https://www.wsj.com/articles/untraceable-bitcoin-is-a-myth-11623860828

OPINION | COMMENTARY

Untraceable Bitcoin Is a Myth

How could the FBI recover $2.3 million of the pipeline ransom? It isn't a mystery.

By Ezra Galston
June 16, 2021 12:27 pm ET

PHOTO: EDGAR SU/REUTERS

Listen to Article (3 minutes) Queue

How did the Justice Department recover $2.3 million of the ransom paid by Colonial Pipeline to a group of hackers known as DarkSide? Isn't bitcoin, the cryptocurrency in which the payment was made, supposed to be untraceable? Actually, no. Bitcoin is anonymous, but it's far from private—an important but often overlooked distinction. The Justice Department recovered more than $1 billion in bitcoin in various investigations during 2020 alone.

The blockchain—bitcoin's historical ledger of all transactions—is publicly viewable at all times by anyone, so that there can't be any under-the-table cash transactions. Software firms such as Chainalysis and Elliptic have supported federal investigators with a suite of analysis tools intended to help trace criminals and tax cheats, including those who try to obscure the bitcoin trail through dozens of successive transactions.

What complicates recovery is bitcoin's anonymity. Senders and recipients are denoted by wallet addresses—a string of numbers and letters—rather than names or Social Security numbers. Other cryptocurrencies such as Monero, zCash and Haven are working on technologies that would offer both anonymity and privacy. But even then, users would face the "off-ramp" dilemma.

That arises when criminals need to spend their bitcoin or convert it into conventional currency. The final transaction deanonymizes the participant and usually triggers the jurisdiction of one or more government agencies. Thus, once criminals transfer their coins into an exchange wallet—even one that doesn't adhere to the exchange's Know Your Customer/Anti-Money-Laundering requirement—investigators have what they need to freeze and ultimately claim those assets. That's likely what happened in the case of Colonial Pipeline.

Traditional currency poses problems of its own for investigators. Bank notes are untraceable unless authorities note the serial numbers in advance. Global banks amassed some $15 billion in fines in 2020 for tacitly enabling money laundering and other financial crimes. Bitcoin's transparency may do more to mitigate fraud and theft than traditional banking and currency ever could.

Mr. Galston is managing partner of Starting Line, an early-stage venture-capital firm, and an investor in bitcoin among other cryptocurrencies.