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.

* * * * * * * *