Understanding the U.S. Role in WeChat, TikTok and Other Chinese Sanctions Targets and How It Affects You and U.S. Businesses

ASIAN CHAMBER OF COMMERCE WEBINAR, MARCH 25, 2021

PRESENTED BY: ROBERT J. WARD, JR.

THE WARD JR LAW FIRM PLLC

Overview

I. Why have WeChat & TikTok been targeted?

II. Why were ZTE & Huawei dealt with differently?

III. Brief Introduction to OFAC

A. The New Non-SDN Communist Chinese Military Companies in Dec. 2020

B. New Sanctions law enactment (CAATSA) in Aug 2017 impacting Russia, Iran, North Korea, and China - implemented Jan 29, 2018.

IV. Review of recent-enforcement actions for lessons learned involving PNB and Schlumberger

V. Discussion on key steps to take to prevent violations including best practices for policies/procedures, screening, due diligence and training.

The content of this presentation is intended for educational and informational purposes only. It does not constitute the provision of legal advice or services by the speaker.

I. Why were WeChat & TikTok targeted?

More Social.
More Fun.

Background on the Trump Admin Concern

In August 2020, Former President Trump issued Executive Orders 13942 (TikTok) and 13943 (WeChat) citing the following:

- Declaration that threats to the information and communications technology and services supply chain by foreign adversaries are a national emergency;

- The Secretary of Commerce to determine whether certain transactions:
  - Pose an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
  - Pose an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
  - Otherwise pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Proposed Regs But for Court Intervention

Proposed Prohibited Transactions:

1. Any provision of services to distribute or maintain the TikTok/WeChat mobile application, constituent code, or mobile application updates through an online mobile application store, or any online marketplace where mobile users within the land or maritime borders of the United States and its territories may download or update applications for use on their mobile devices;

2. Any provision of internet hosting services enabling the functioning or optimization of the TikTok/WeChat mobile application, within the land and maritime borders of the United States and its territories;

3. Any provision of content delivery services enabling the functioning or optimization of the TikTok/WeChat mobile application, within the land and maritime borders of the United States and its territories;

4. Any provision of directly contracted or arranged internet transit or peering services enabling the functioning or optimization of the TikTok/WeChat mobile application, within the land and maritime borders of the United States and its territories;

5. Any provision of services through the TikTok/WeChat mobile application for the purpose of transferring funds or processing payments to or from parties within the land or maritime borders of the United States and its territories; and

6. Any utilization of the TikTok/WeChat mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the land and maritime borders of the United States and its territories.

What the Courts Did (Trump Admin Appealed both orders)

On the TikTok Order:

A federal district court in E.D. Pennsylvania issued a nationwide preliminary injunction on 10/30/2020 in the case of Douglas Marland et al. v. Trump et al., No. 20-cv-4597. The Court granted the Plaintiffs' motion for an injunction against the implementation of Executive Order 13942 (limited to the Secretary of Commerce's Identification of Prohibited Transactions 1 through 6, **TikTok/ByteDance**).

On the WeChat Order:

A federal district court in N.D. California issued a nationwide preliminary injunction at on 9/19/2020 in the case of WeChat Users Alliance v. Trump, No. 20-cv-05910-LB. The Court granted the Plaintiffs' motion for an injunction against the implementation of Executive Order 13943 (limited to the Secretary of Commerce's Identification of Prohibited Transactions 1 through 6, **WeChat/Tencent**).

Where Things Stand with Pres. Biden

On February 10th (respecting the TikTok case) and on February 11th (respecting the WeChat case), the Biden administration asked the federal appeals courts to place a hold on proceedings surrounding the Trump administration's attempted bans on the two social media apps.

In the Ninth Circuit Court of Appeals filing (covering the WeChat Case), the Biden administration explained in their proceedings as follows:

- "The Department [of Commerce] plans to conduct an evaluation of the underlying record justifying those prohibitions. The government will then be better positioned to determine whether the national security threat described in the President's August 6, 2020 Executive Order, and the regulatory purpose of protecting the security of Americans and their data, continue to warrant the identified Prohibitions"

Will this withstand conservative scrutiny?

Conservatives believe Trump made the correct national security call, as reported here (https://www.washingtonpost.com/technology/2021/02/11/wechat-trump-biden-pause/), because both apps collected "vast swaths" of data on Americans and offered the Chinese Communist Party avenues for censoring or distorting information.

Meanwhile, the Biden administration is already hedging its bets (via reporting in the same Washington Post article cited above) by asserting:

". . . that the Biden administration 'remains committed to a robust defense of national security as well as ensuring the viability of our economy and preserving individual rights and data privacy.'"

II. Why were ZTE and Huawei Dealt with Differently?

Both Huawei and ZTE Corp. have faced trouble with the U.S. and other governments over dealings with Iran and fears the Chinese companies' equipment might be used for spying. ZTE was nearly driven out of business in 2017 when Washington barred it from buying U.S. technology over exports to North Korea and Iran.

What was different was how the U.S. Government dealt with each of them. Both were added to the Commerce Bureau of Industry and Security (BIS)Entity List. Huawei, however, also confronted an arrest and prosecution of a C-Suite executive.

OFAC SDNs should not be confused with the BIS Denied Persons and Entities Lists

- The Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce maintains separate lists for the purposes of the programs that it administers (including the Denied Persons List and the Entity List).
- The Denied Persons List consists of individuals and companies that have been denied export and re-export privileges by BIS.
- The Entity List consists of foreign end users who pose an unacceptable risk of diverting U.S. exports and the technology they contain to alternate destinations for the development of weapons of mass destruction (e.g., ZTE, Huawei and affiliates).
- Accordingly, U.S. exports to those entities may require a license. Authority for the Denied Persons List and the Entity List can be found in Title 15, Part 764, Supplement No. 2 and Title 15, Part 744, Supplement No.4 of the U.S. Code of Federal Regulations, respectively.

Specially Designated Nationals (SDNs)

- Prohibitions against specific named individuals and entities (the “black list”).
- The names are incorporated into OFAC’s list of Specially Designated Nationals and Blocked Persons ("SDN list") which includes thousands of names of companies and individuals who are connected with the sanctions targets.
- For Global Companies, it is critical to set up a system for pre-screening transactions to ensure no business is conducted with such blocked persons; requires asset freezing.
- OFAC does not maintain the only blacklist; in fact, there are numerous other lists that should be screened for any company contemplating going global.
- If screening for SDNs is new for you, please see my article in the SCCE May 2015 Compliance & Ethics Professional Magazine: “OFAC’s global sanctions: A greater headache than the FCPA?”

The ZTE Case – The Prohibited Conduct

- From January 2010 to about March 2016, ZTE engaged in: **(i)** the exportation, sale, or supply, directly or indirectly, from the United States of goods to Iran or the Government of Iran; **(ii)** the reexportation of controlled U.S.-origin goods from a third-country with knowledge that the goods were intended specifically for Iran or the Government of Iran; and **(iii)** activity that evaded or avoided, attempted and/or conspired to violate, and/or caused violations of the ITSR prohibitions.

- From about January 2010 to March 2016, ZTE's highest-level management developed, approved, and implemented a company-wide plan to conceal and facilitate ZTE's illegal business with Iran. ZTE's highest-level management was specifically aware of and considered the legal risks of engaging in such activities prior to signing contracts with Iranian customers. Essential to the performance of such contracts was ZTE's procurement of and delivery to Iran of U.S.-origin goods, including goods controlled for anti-terrorism, national security, regional stability, and encryption item purposes. Pursuant to its contracts with Iranian customers, ZTE was required to and did in fact enhance the law enforcement surveillance capabilities and features of Iran's telecommunications facilities and infrastructure.

- ZTE's unlawful business activities with Iran were publicly disclosed in a media report in 2012. Shortly thereafter, ZTE learned of the U.S. government's investigation into the company's business activities with Iran. ZTE subsequently communicated to the U.S. government that it had wound down and ceased its Iran-related activities. However, ZTE's highest-level leadership decided to resume its Iran-related business in 2013, which it continued until 2016, when the Commerce Dept. suspended the company's export privileges by adding it to the Entity List. Under the direction of its leadership, ZTE deleted evidence and provided the U.S. government with altered information to hide the fact that it had resumed its unlawful business with Iran.

Lessons Learned from ZTE

Lesson 1 -> Don’t lie and Don’t create false/misleading records!

Lesson 2 -> Don’t destroy evidence!

Lesson 3 -> Don’t rely on non-disclosure agreements to cover-up crimes!

Lesson 4 -> Don’t restart your criminal activity during the investigation!

Lesson 5 -> Don’t create a written, approved corporate strategy to systematically violate the law!

Lesson 6 -> Don’t lie about reprimanding involved employees only to provide 35 of them with bonuses!

ZTE settlement

The United States government agreed to a $1,000,000,000 fine and a change in leadership of ZTE, including its Board of Directors on March 17, 2017 in exchange for taking ZTE off the entity list.

Additionally, the US required the company to institute a comprehensive compliance department with the appointment of a monitor. Specifically, ZTE had to submit to a three-year period of corporate probation, during which time an independent corporate compliance monitor reviewed and reported on ZTE's export compliance program. ZTE was also required to cooperate fully with the Department of Justice (DOJ) regarding any criminal investigation by U.S. law enforcement authorities.

The Huawei Entity Listing

BIS added Huawei Technologies Co., Ltd. (Huawei) and many of its non-U.S. affiliates to the Entity List effective May 16, 2019.

It did so with information that provided a reasonable basis to conclude that Huawei was engaged in activities that are contrary to U.S. national security or foreign policy interests and its non-U.S. affiliates pose a significant risk of involvement in activities contrary to the national security of the United States. This information included alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions.

Effective August 19, 2019, BIS added another 46 non-U.S. affiliates of Huawei to the Entity List because they also pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States.

Practical Impact of Being on the Entity List

The addition of Huawei and its affiliates to the Entity List imposed a license requirement in addition to those found elsewhere in the Export Administration Regulations (EAR).

Specifically, the additions imposed a license requirement for all items subject to the EAR. Therefore, the export, reexport, or transfer (in-country) of any item subject to the EAR to Huawei or any of its listed affiliates now requires a license unless the activity is authorized pursuant to the Entity List rule's savings clause.

All other exports, reexports, or transfers (in-country) of items subject to the EAR will require a license and the U.S. Government will review license applications for such transactions under a presumption of denial.

Meanwhile on February 8, 2021 Huawei filed a lawsuit in the U.S. Court of Appeals for the Fifth Circuit disputing the FCC's designation of Huawei as a national security threat.

Remember What Happened to Huawei Technologies CFO?

CFO Meng Wanzhou, who is also deputy chairman of the board and the daughter of Huawei founder Ren Zhengfei, was arrested December 2018 in Vancouver, Canada on an U.S. extradition request. Specifically, she is alleged to have committed bank fraud for allegedly misleading HSBC* Holdings Plc about Huawei's business dealings in Iran, causing the bank to break US sanctions.

Meng remains under house arrest on bail in Vancouver (with an ankle tracking bracelet).

Her case is scheduled to wrap up in April 2021 as US prosecutors are discussing a deal with her lawyers to resolve criminal charges against her.

* HSBC's OFAC violations amounted to the bank paying an $875 million dollar fine (https://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx).

U.S. Fight against Huawei has Adversely Impacted Canada

Meng's arrest has soured relations between Canada and China.

In apparent retaliation, China detained former Canadian diplomat Michael Kovrig and Canadian entrepreneur Michael Spavor. Kovrig and Spavor remain jailed. Meng remains free on bail in Vancouver and living in a mansion.

China also handed death sentences to four Canadians convicted of drug smuggling.

China has also placed restrictions on various Canadian exports to China, including canola oilseed.

What is the U.S. concern over Huawei otherwise?

The United States has been lobbying allies to avoid using Huawei equipment in their next-generation mobile telecommunications systems, known as 5G. Washington argues China could use the technology to attack critical infrastructure and compromise intelligence sharing.

The new Biden administration plans to continue to apply restrictions to Chinese technology transactions generally involving critical U.S. infrastructure, networks and satellite operations, large data hosting operations, widely used internet connectivity software, and technology used in advanced computing, drones, autonomous systems or advanced robotics.

https://www.wsj.com/articles/u-s-to-impose-sweeping-rule-aimed-at-china-technology-threats-11614362435

III. Intro to OFAC

OFAC

OFFICE OF FOREIGN ASSET CONTROL

(AS THE U.S. APPETITE FOR FOREIGN INTERVENTION WANES, OFAC IS BECOMING A TOOL OF CHOICE)

Key Questions to Ask Regarding Risk:

1) Does my business cater to a global audience (or even a significant domestic audience, as there is an increasing threat of domestic terrorism)?

2) Does my business make use of the U.S. financial system?

3) Does my business involve the Defense or Oil & Gas industries?

4) If any of the above are "yes", does my business conduct screening of business partners?

How a Sanctions Program Begins

- Most sanctions, though rooted in statutes (e.g., The Trading with the Enemy Act), begin through Executive Orders (EOs).
- The President *declares* a national emergency to address an unusual and extraordinary threat.
- Such threats have their source in whole or in substantial part outside the U.S.
- The *threat* is to the national security, foreign policy, or economy of the U.S. and can include:
  - Nuclear, biological, or chemical missile proliferation,
  - Human rights abuses, and
  - Interference with democratic processes and other "hacking"/digital espionage threats.
- The President's declaration is a requirement for invoking the International Emergency Economic Powers Act (IEEPA) authority.
- For long-term sanctions programs, regulations and interpretive guidance follow EO issuance.

The Content of Executive Orders

- Declare the conditions are met for the imposition of sanctions
- Establish the sanctions program
- Provide guideposts for agency action
- May include designation of persons or entities to a prohibited blacklist (more below)
- "Blocks" property and interests in property in the U.S. that enter the U.S. (tangibly and intangibly), or that are or come within the possession or control of a U.S. person
- Effect of blocking an asset – it may not be "transferred, paid, exported, withdrawn, or otherwise dealt in"
- URL: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

OFAC Penalties*

Criminal Penalties for a Willful Violation ->	Fines Up to $20 million and up to 30 years in prison. [21 U.S. Code § 1906 and 50 U.S. Code § 1705]
Civil Penalty Violation of the IEEPA->	$311,562 or twice the amount of the underlying transaction.
Civil Penalty Violation of the Trading With the Enemy Act ->	Up to $91,816 for each violation.
Civil Penalty Violation of the Foreign Narcotics Kingpin Designation Act ->	Up to $1,548,075 for each violation.

* Just amended March 17, 2021; please see: https://home.treasury.gov/system/files/126/fr2021_05506.pdf

OFAC's Jurisdiction

U.S. Persons

United States person means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any person in the United States.

The law applies no matter where such U.S. person is located.

Dealing in Property Interests

Sanctions prohibit U.S. persons from "dealing in property interests: of a sanctioned country or blacklisted individual or entity."

Property includes anything tangible or intangible, including money, trade, checks, contracts, goods, real property, contingent rights or obligations.

Extraterritorial Applications

Entity organized under the laws of the United States includes *foreign branches*. U.S. controlled foreign subsidiaries are also captured under some sanctions programs.

Under the Iran Threat Reduction and Syria Human Rights Act (ITRA), similar to the law already in effect regarding Cuba, a US person "owns or controls" a foreign entity if it: (1) *holds more than 50 percent* of the equity interest by vote or value in the entity; (2) holds a majority of seats on the board of directors of the entity; *or* (3) otherwise controls the actions, policies, or personnel decisions of the entity.

New Sectoral Sanctions Identification List (SSI) entity 33% Rule applies in the O&G sector per the Countering America's Adversaries Through Sanctions Act (CAATSA) respecting Russia

OFAC Prohibitions Against Evasion & Facilitation

EVASION/AVOIDANCE

A US person transaction that evades or avoids any sanction/prohibition or attempts to do so is itself a violation.

For example, changing processes and procedures that formerly required U.S. person approval so they can occur without U.S. participation would be an unlawful evasion.

FACILITATION

A U.S. person's facilitation of an exportation or re-exportation of goods, technology or services to or from a sanctioned target is prohibited.

For example, brokering deals or sales or providing freight forwarding services.

Know Your Customer!

Facilitation is a broad concept that captures anything reasonably determined to aid or abet a violation. For example, in the *Sea Tel, Inc.* case, an export occurred to S. Korea with knowledge or reason to know the products would be re-exported to Iran. Proper Due Diligence is Now Critical!

List of OFAC Sanctions Programs

ACTIVE SANCTIONS PROGRAMS:	PROGRAM LAST UPDATED:
Balkans-Related Sanctions	02/03/2017
Belarus Sanctions	12/23/2020
Blocking Property of Certain Persons Associated with the International Criminal Court Sanctions	09/30/2020
Burma-Related Sanctions	03/25/2021
Burundi Sanctions	06/02/2016
Central African Republic Sanctions	08/07/2020
Chinese Military Companies Sanctions	03/14/2021
Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA)	03/02/2021
Counter Narcotics Trafficking Sanctions	03/03/2021
Counter Terrorism Sanctions	03/25/2021
Cuba Sanctions	12/21/2020
Cyber-Related Sanctions	03/02/2021
Democratic Republic of the Congo-Related Sanctions	03/10/2021
Foreign Interference in a United States Election Sanctions	01/11/2021
Global Magnitsky Sanctions	03/25/2021
Hong Kong-Related Sanctions	03/17/2021
Iran Sanctions	03/05/2021
Iraq-Related Sanctions	12/23/2020
Lebanon-Related Sanctions	07/30/2010
Libya Sanctions	08/06/2020
Magnitsky Sanctions	12/10/2020
Mali-Related Sanctions	02/06/2020
Nicaragua-Related Sanctions	12/21/2020
Non-Proliferation Sanctions	03/02/2021
North Korea Sanctions	12/08/2020
Rough Diamond Trade Controls	06/18/2018
Somalia Sanctions	07/10/2020
Sudan and Darfur Sanctions	08/11/2020
South Sudan-Related Sanctions	02/26/2020
Syria Sanctions	12/22/2020
Syria-Related Sanctions	12/22/2020
Transnational Criminal Organizations	07/22/2019
Ukraine-/Russia-Related Sanctions	03/02/2021
Venezuela-Related Sanctions	02/02/2021
Yemen-Related Sanctions	03/02/2021

Lists Against which to Conduct Screening

- For global companies, at a minimum, the followings lists should be checked:

Source	Description	Updated On	# Records
OFAC	(SDN) Specially Designated Nationals List	03/25/21	38,239
	(OFCL) Consolidated List	03/18/19	1,976
BIS	BIS Denied Persons/Unverified List/Entity List	02/04/21	5,328
Canada	Public Safety List	02/04/21	1,579
UK	HM Treasury Sanction List	03/24/21	11,153
UN	United Nations Consolidated List	02/25/21	6,279

Types of Sanctions-Programs

- **Country Based** – prohibits a broad spectrum of activities based on the country
  - Cuba, Iran, North Korea, Syria, *Crimea*
- **Targeted Sanctions** – imposed on specific individuals, entities or activities within a country:
  - Ukraine related, Belarus, Venezuela, Lebanon, Somalia
- **Activity Based** – sanctions people or based on certain activities:
  - Cyber-related, Rough Diamond, Magnitsky, Crypto-currencies
- **Inter-Department Based** – Commerce's April 28, 2020 expansion of export, re-export, and transfer (in-country) controls for Military End Use or End Users in China, Russia or Venezuela
- **Investment Prohibitions** – Certain designated Chinese companies deemed to be involved in developing China's military capabilities – Divestment required by November 11, 2021 - https://www.sec.gov/files/risk-alert-securities-investments-finance-communist-chinese-military-companies.pdf
- **Surveillance Equipment Bans** - via the National Defense Authorization Act – as of August 2019, all federal government bodies should have started on plans to remove tech from four manufacturers (Huawei, ZTE, Dahua and Hikvision) considered too closely linked to the Chinese government - https://www.forbes.com/sites/thomasbrewster/2019/08/21/2000-banned-chinese-surveillance-cameras-keep-watch-over-us-government-sites/?sh=588b34f97f65

III. A. New Non-SDN Menu-Based Sanctions

NON-SDN COMMUNIST CHINESE MILITARY COMPANIES LIST (NS-CCMC LIST)

NON-SDN MENU-BASED SANCTIONS LIST (NS-MBS LIST)

Which Chinese Companies are Deemed to be Inextricably tied to the Chinese military?

- Check this link: https://www.treasury.gov/ofac/downloads/ccmc/ns-ccmc_list.pdf
- Companies I've had to counsel clients on the list are:
  - **Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision) Hikvision Hangzhou Hikvision Digital Technology Co Ltd 002415 CN**
  - **Huawei Huawei Investment & Holding Co Ltd KMC**
  - **Note: ZTE is Not on the List** (due to successful settlement of its case and continued compliance)
- Some on the list that will impact Houston's chief industry
  - **China National Offshore Oil Corp. (CNOOC) China National Offshore Oil Corp CNOZ CN CNOOC Limited CEO US / 883 HK / CNU CA**
  - **Sinochem Group Co Ltd Sinochem Group Co Ltd 1001Z CN**
- Others on the list indicating a cybersecurity concern:
  - **China Communications Construction Company (CCCC) China Communication Construction Group Company, Ltd. China Communications Construction Co Ltd 601800 CN / 1800 HK**
  - **China Mobile Communications Group China Mobile Communications China Mobile Communications Group Co Ltd CHMOBZ CN China Mobile Limited CHL US / 941 HK China National Chemical Corporation (ChemChina) China National Chemical Corp Ltd CHNCCZ CN**
  - **China Telecommunications Corp. China Telecommunications China Telecommunications Corp CNTELZ CN China Telecom Corporation Limited CHA US / 728 HK**
  - **China United Network Communications Group Co Ltd China United Network Communications Ltd 600050 CN China Unicom (Hong Kong) Limited CHU US / 762 HK**
- Other Key Industries include aerospace, electronics, semiconductors and heavy construction
- On January 13, 2021, it was announced that Alibaba, Baidu and Tencent would not be added to the investment-prohibition list of those Chinese companies supporting the Chinese military (U.S. Won't Ban Investments In Alibaba, Tencent, Baidu–But 9 Other Firms Are Set To Be Off Limits (forbes.com))

Divestment Timelines under EO 13959

Identified	Effective Date	Divestment Date
31 companies initially identified by the DoD in June and August 2020	11 January 2021	11 November 2021
4 companies identitied by the DoD on 3 December 2020	1 February 2021	3 December 2021
4 companies identified by OFAC on 8 January 2021	9 March 2021	8 January 2022
9 companies identified by the DoD on 14 January 2021	15 March 2021	14 January 2022

Xiaomi wins Stay of Execution on Trump era CCMC Executive Order

- Xiaomi Communications Co., Ltd. sued the U.S. Government in Federal District Court in January 2021, arguing there is insufficient evidence for its inclusion on the list of "Communist Chinese Military Companies" (CCMC).
- The Government cited Xiaomi founder Lei Jun's recognition as an "Outstanding Builder of Socialism with Chinese Characteristics" by a Chinese ministry and the company's investment in 5G and artificial intelligence as the main grounds for alleging Xiaomi had ties with the People's Liberation Army. Please see: https://on.ft.com/3eLybcY
- Xiaomi argued irreparable harm due to its inclusion on the CCMC list as it would have barred U.S. investors from owning shares, potentially triggering delisting from U.S. exchanges and deletion from global benchmark indices.
- U.S. District Judge Rudolph Contreras granted a temporary halt on Friday March 12, 2021 stating the U.S. case against Xiaomi was "deeply flawed".
- Luokung Technology Corp. also filed a motion for a temporary restraining order in Federal District Court on March 5, 2021. Please see: https://www.luokung.com/en/press/121.html
- More similar lawsuits are likely to follow.

NDAA mandating surveillance tech ban

- Surveillance Equipment Bans - via the Sen. John McCain National Defense Authorization Act 2018
- Three stages:
  - the 'procurement ban', which bans federal procurement of covered equipment/service and went into effect in August 2019
  - the 'blacklist clause', which bans federal agencies from doing business with those who "use" covered equipment/services and went into effect in August 2020 – "Reasonable Inquiry" Required
  - the 'funding ban', which prohibits federal dollars from being spent on covered goods/services and went into effect in August 2020
- As of August 2019, all federal government bodies should have started on plans to remove tech from four manufacturers (Huawei, ZTE, Dahua and Hikvision) considered too closely linked to the Chinese government – However, this was already proving difficult even for the Government to undertake https://www.forbes.com/sites/thomasbrewster/2019/08/21/2000-banned-chinese-surveillance-cameras-keep-watch-over-us-government-sites/?sh=588b34f97f65

III. B. Countering America's Adversaries Through Sanctions Act

Passed and signed into law in August 2017 respecting Russia, North Korea, Iran and China

Quote from U.S. Senator Bob Corker (R-Tenn.), chairman of the Senate Foreign Relations Committee (July 27, 2017).

"With near unanimous support in both chambers of Congress, this legislation sends a strong signal to Iran, Russia and North Korea that our country will stand firm and united in the face of their destabilizing behavior."

Key Dates

- July 25, 2017: Passed the House of Representatives 419 to 3
- July 27, 2017: Passed the Senate 98 to 2
- August 2, 2017: Signed by President Trump (a presidential veto would have been easily overridden otherwise)

Quote from President Trump (August 3, 2017).

“The bill remains seriously flawed -- particularly because it encroaches on the executive branch's authority to negotiate."

"Congress could not even negotiate a health care bill after seven years of talking. By limiting the executive's flexibility, this bill makes it harder for the United States to strike good deals for the American people, and will drive China, Russia, and North Korea much closer together."

"I built a truly great company worth many billions of dollars. That is a big part of the reason I was elected. As President, I can make far better deals with foreign countries than Congress."

Key Objectives

- Codifies and expands sanctions for Russia's annexation of Crimea, continuing destabilization in Eastern Ukraine and interference in the U.S. presidential election
- Limits the president's authority to terminate or modify the Russia sanctions (Efforts by the President to relax, suspend, or terminate the Russia-related sanctions currently in effect will be subject to mandatory review by Congress).
- Expands sanctions against Iran and North Korea
- Used as the basis for the CCMC investment prohibitions (also, the IEEPA & NDAA)
- On 12/07/2020, President Joe Biden's national security adviser said the incoming administration wants to put Iran "back into the box" by rejoining the nuclear deal and forcing Tehran to comply with the terms of the original agreement. https://www.wsj.com/articles/biden-national-security-adviser-sees-u-s-rejoining-iran-nuclear-deal-11607399179

Immediate Impact

- New additions to various blacklists. – e.g., OFAC Specially Designated Nationals (SDN) list - OFAC Sectoral Sanctions Identifications (SSI) list – Commerce's BIS Entity List ->

INCREASED IMPORTANCE OF REAL-TIME SCREENING

- New or modified black-listed party end-use and financing restrictions ->

INCREASED DUE DILIGENCE REQUIRED

- New sanctions on foreign persons who provide support to Russia SDNs or prohibited end-uses or activities ->

INCREASED OWNERSHIP ANALYSIS REQUIREMENTS [50% AND NEW 33% O&G INDUSTRY OWNERSHIP RULES]

Biden to Focus on Multilateral Front to China (1)

- Biden has vowed to revitalize American alliances and work towards multilateral solutions to global challenges. The meeting of the Quad (U.S., India, Japan and Australia) was 3/12/2021.
- The core issue uniting the group is maritime security in the Indian and Pacific oceans. That agenda includes joint naval exercises, disaster relief, anti-piracy efforts and environmental initiatives.
- Please see: Joe Biden Won't 'Pull Any Punches' on China, State Department Says Before Pivotal Talks (newsweek.com)
- Please also see: Quad grouping will become central part of the U.S. strategy in Asia - The Washington Post

Biden to Focus on Multilateral Front to China (2)

- Fresh off the Press from Monday 03/22/2021: the adoption of coordinated Xinjiang-related sanctions by Canada, the EU, the UK, and the United States. The PRC Ministry of Foreign Affairs responded by announcing sanctions on ten EU individuals and four entities.
- The US State Department published an update to its October 2020 report under Section 5(a) of the Hong Kong Autonomy Act (HKAA), identifying an additional 24 PRC and Hong Kong officials. (The October 2020 report identified 10 officials.) Under Section 5(b) of the HKAA, the US Treasury Department has 30 to 60 days to identify any foreign financial institution that knowingly engages in a "significant transaction" with one of the 24 individuals.
  - What's the big deal over the State Department's Section 5(a) update on 03/18/2021? These same persons were previously sanctioned under Executive Order 13936 in November and December 2020 and January 2021.
  - That means banks would have identified them all already.
  - It appears the report was intended to send a message before the 03/18/2021 US-PRC summit in Alaska that the Biden administration intends to remain tough. Time will tell with OFAC's forthcoming Section 5(b) report in about 30 to 60 days. In the first round, OFAC issued a null report; the second round will likely involve identification of complicit foreign financial institutions.

IV. Key OFAC Cases For Lessons Learned

PNB Paribas, Schlumberger, ZTE, Apple, Amazon and Bitgo

PNB Paribas – largest OFAC civil penalty

- In June 2014, BNP Paribas SA [BNPP] agreed to pay OFAC $964 million (out of a total of almost $9 billion in civil penalties to US regulators for various offenses).
- The settlement agreement details numerous instances of facilitation and concealment all of which BNPP's subsidiary in Geneva and branch in Paris overwhelmingly conducted in violation of U.S. sanctions laws.
- Those instances of facilitation and concealment included omitting references to sanctioned parties; replacing the names of sanctioned parties with BNPP's name or a code word; and structuring payments in a manner that did not identify the involvement of sanctioned parties in payments sent to U.S. financial institutions.

Chief Lessons Learned in the PNPP case

- A failure to recognize that foreign office facilitation and sanctions evasion activities that still make use of the U.S. intermediary banks in New York City in processing U.S. dollar wire transfers will constitute OFAC violations.
- Because of BNPP's presence in the United States and continued desire to make use of the U.S. dollar reserve currency in its international commercial operations,
  - BNPP was subject to OFAC jurisdiction,
  - The bank was forced to pay heavy fines for its egregious facilitation and evasion activities, and
  - All to retain its player status in the U.S. financial market.

The Schlumberger Case

SCHLUMBERGER PROHIBITED CONDUCT

- On March 25, 2015, Schlumberger settled its OFAC criminal case in the amount of $232.7 million (largest OFAC criminal penalty yet). Schlumberger's US Drilling & Measurements (D&M) did the following:

(1) approving and disguising the company's capital expenditure requests from Iran and Sudan for the manufacture of new oilfield drilling tools and for the spending of money for certain company purchases (D&M personnel outside the United States referred to Iran as "Northern Gulf" and Sudan as "Southern Egypt" or "South Egypt" in their email communications with D&M personnel in the United States);

(2) making and implementing business decisions specifically concerning Iran and Sudan (that is, D&M headquarters personnel made and implemented business decisions in the day-to-day operations of Iran and Sudan); and

(3) providing certain technical services and expertise in order to troubleshoot mechanical failures and to sustain expensive drilling tools and related equipment in Iran and Sudan (that is, at times, queries entered by, or on behalf of, D&M personnel in Iran and Sudan were addressed by D&M personnel located in the United States).

Lessons Learned from Schlumberger

SCHLUMBERGER LESSONS LEARNED

- Schlumberger, though incorporated outside the United States, managed to violate U.S. sanctions laws by involving persons (including non-US citizens or residents), affiliates, unaffiliated business partners or facilities located in the United States.
- Any involvement in sanctioned country activities by a person or entity (whether an affiliate or not) within the United States, or by US citizens or residents anywhere in the world, may trigger liability for a foreign company that itself has no direct presence in the United States but which benefits from those facilitated activities.
- Schlumberger underwent a three-year probationary period and was required to hire an independent consultant to review its sanctions compliance program.

V. Best Practices for Avoiding OFAC Violations

Best Practices for policies and procedures, screening, due diligence and training.

Best Practices for Policies and Procedures

- If you're operating globally or *even only domestically*, you absolutely need policies and procedures, even if made a mere part of your Export Control and Anti-Boycott Compliance policies and procedures.
- Provide Annual Training that Includes Certification on Having Read the Policies. "Morgan Stanley" FCPA case (Director of Ops in China bribed left and right, but company protected due to training).
- The policies and procedures should designate a responsible party/department, e.g. international trade compliance department or even the chief compliance officer who can issue a STOP order.
- The policies and procedures should provide an up-to-date overview of the sanctions programs impacting the company's operations (not to mention discuss all country-wide embargoes so personnel know when they must refrain from facilitating).
- The policies and procedures should provide contract clause model language (including destination control statements to prevent unauthorized diversion).
- Please see OFAC's Framework for a Proper Sanctions Compliance set of Policies and Procedures published May 2019: framework_ofac_cc.pdf (treasury.gov)

Screening Best Practices

- A Best in Class Screening practice is one that is fully automated and internalized in the company's ERP system, including an automated block imposed for potential black-list matches (high volume big companies such as banks and Fortune 500 companies have this level of screening sophistication).
- Just the same, some algorithmic search capability for alias names is recommended ("Fuzzy Logic").
- Even for companies with a limited budget but poised to launch globally, OFAC provides an updated screening tool link on its website at no cost as follows (Update from 01/25/2021 respecting fuzzy logic upgrade: https://content.govdelivery.com/accounts/USTREAS/bulletins/2bd0d02)
  - https://sanctionssearch.ofac.treas.gov/
- A good free check to ensure coverage of key U.S. Government blacklists (no fuzzy logic) is via: Consolidated Screening List (trade.gov)
  - The Consolidated Screening List is a searchable and downloadable file that consolidates export screening lists of the Departments of Commerce, State and the Treasury into one spreadsheet to assist in screening potential parties to regulated transactions.
  - If the potential match is from the consolidated list, please follow the detailed instructions on the Consolidated List homepage to determine what list the potential match is from and under what government agency's jurisdiction.
- There are vendors that provide such alias search capability that are cost effective, including a free service: http://www.instantofac.com/ as well as an inexpensive option with guaranteed updates at: http://ofacanalyzer.com/
- Audit Trail recordation via the chosen system is highly recommended.

Best Practices for Due Diligence

- Conduct a Risk Assessment on Vulnerabilities for your Company.
- Ask yourself these questions:
  - Do you do business with third parties in known transshipment cities such as Dubai, Hong Kong, Istanbul, or Singapore?
  - Is your industry known for involvement in countries neighboring embargoed countries where diversion could easily occur? Chinese locations in proximity to N. Korea?
  - Do you have sensitive goods, technologies and services with both civilian/military dual-use applications?
  - What is your process for intervention if and whenever needed? Stop order? Is it effective? Do contracts excuse performance for true match discoveries?
- Vendor/Customer Set-Up Due Diligence is critical for OFAC sanctions in addition for FCPA concerns.
- Global Trade Compliance Questionnaire for vetting new export customers and supply chain is critical.
- For screening on business and transaction partners, is your chosen system capable of handling the volume without overly disrupting the business?
- Does your system screen for potential aliases?
- What is your standard for gauging a false positive versus a match when screening for aliases?
- On the 50% rule respecting the Iranian, Ukraine (33% rule for the O&G industry) related sanctions etc., what is your process for uncovering entity ownership?
- Can you independently verify ownership? Dow Jones offers a service for this. If not or if inadequate info is provided, are transaction stops imposed?
- Is there a clear escalation process when issues arise?
- When is enough due diligence enough?

Robert J. Ward, Jr. Contact Info

Robert J. Ward, Jr.

Attorney-At-Law

The Ward Jr Law Firm PLLC

Phone: +1-281-728-4036

Email:

robertjwardjr@gmail.com

Websites:

https://thesanctionsgeek.com/

HIBC - Houston International Business Corp. (energy-environment.com)