Miller & Chevalier

US Export Controls and Economic Sanctions Enforcement: Seven Trends to Watch in 2018

If 2017 was a busy – and possibly landmark – year for export control and sanctions enforcement, 2018 may prove even more remarkable. And so, as the Trump Administration consolidates its positions and policies, what trends can trade compliance professionals expect to characterise 2018? Tim O'Toole looks into his crystal ball and offers his predictions.

Timothy P. O'Toole
Member
totoole@milchev.com
202.626.5552

Trying to predict US export controls and economic sanctions enforcement trends can be a slippery business, especially when the leadership at US enforcement agencies is going through a period of significant change. Nonetheless, based on what we have already seen from the new administration, and what we have consistently seen over the past few years from the US government's export controls and economic sanctions enforcement agencies, the following seven trends seem likely to dominate the export controls and sanctions landscape for the foreseeable future.

Trend One: Iran has been and will likely remain the US enforcement focus

Recent headlines have highlighted the new administration's change in policy toward the Iran Nuclear Deal (officially known as the Joint Comprehensive Plan of Action or 'JCPOA'). From those headlines, a reader could come away believing that the previous administration had been 'soft' on Iran, but the new one is taking a harder line. This story line is a bit simplistic, however, because although the previous administration did (along with the rest of the world community) enter into the JCPOA, its enforcement of the Iran sanctions remained the highest priority over at least the past five years.

That priority has remained steady into the new administration. In March 2017, the new Commerce Secretary, Wilber Ross, personally announced the most significant penalty ever for the reexport of US-origin goods to Iran, $1.2 billion, in a criminal and civil action brought against Chinese telecommunications company Zhongxing Telecommunications Equipment Corporation ('ZTE') and its subsidiaries. The penalty was imposed after a joint investigation by the Commerce Department's Bureau of Industry and Security ('BIS'), the Treasury Department's Office of Foreign Assets Control ('OFAC'), and the US Department of Justice ('DOJ').

The nature of the underlying conduct in the ZTE action is significant because, while US enforcement agencies had previously imposed such enormous penalties against foreign financial institutions that utilised the US financial system in the Iran trade, they had never before imposed a similarly large penalty based on the sale by a foreign company of US-origin goods to Iran. The announcement potentially signalled a new era for US enforcement of the Iran embargo, putting companies around the world on notice – even after the JCPOA – of the serious risk posed by the resale of US-origin goods to Iran. The ZTE enforcement action also reaffirms a long-standing message from BIS, OFAC, and DOJ about the risks of affirmatively concealing transactions with sanctioned jurisdictions from US enforcers. Such concealment, as it had in connection with previous sanctions against foreign financial institutions, factored heavily into the size and the scope of the ultimate remedy.

The ZTE penalty was one of a host of recent enforcement actions taken by US regulators in connection with the US embargo on Iran. Over the Summer and into the Fall of 2017, US enforcers resolved a series of matters related to the Iran sanctions, imposing penalties against US insurer AIG for insuring Iran (and other) transactions in violation of US embargoes, and for

failing to scrutinise its policies to ensure that they excluded such insurance. OFAC also imposed a significant fine against a company that shipped used cars through Iran on the way to Afghanistan (American Export Lines) and another against a Chinese oil and gas company (China Oilfield Services Limited or 'COSL') that supplied US-origin goods to Iranian oil fields. OFAC also imposed several other penalties against US parent companies that had attempted to allow their subsidiaries to conduct lawful business in Iran, but had participated in that business nonetheless, through supervising or otherwise facilitating Iran transactions.

Finally, in perhaps the most significant post-ZTE enforcement action, US regulators imposed a $12 million civil penalty against two Singapore companies, CSE Global/CSE Transtel, which used US dollar accounts in Singapore to process transactions arising out of otherwise lawful telecommunications equipment sales to Iran. As we discuss more fully below, this enforcement action took a very broad jurisdictional theory applying US sanctions to Iran-related sales that did not involve US-origin goods, were lawful in the country of origin, and the Iran transactions themselves were not processed through the US financial system.

Such a jurisdictional theory is even broader than the one the US is pursuing in a criminal prosecution in New York involving Turkish bankers Reza Zarrab and Mehmet Atilla who allegedly used the US banking system to process Iranian transactions that otherwise had no connection to the United States. The trial court has upheld such a theory. In the event convictions are obtained, it is likely that that ruling will be scrutinised on appeal.

Taken together, these enforcement actions make clear that the Iranian embargo will remain the top priority of US enforcers for the foreseeable future. Violations of the US sanctions against Iran remain the source of the most significant fines and many criminal prosecutions. Indeed, as tension surrounding the JCPOA continues to rise, it seems likely that US regulators will, if anything, intensify their focus on Iran.

Trend Two: Targeted enforcement actions against a growing number of industries

Another trend to watch is the nature of the industries being targeted by US enforcers. For several years, OFAC, BIS, and DOJ have focused largely on the world financial community and the oil and gas industry. This focus remained true in 2017, when penalties were again imposed against several oil and gas companies, mostly in connection with drilling operations in Iran that involved US-origin goods, and against financial institutions that utilised the US financial system to process transactions with embargoed countries.

But the real enforcement story of 2017 was the expansion of significant penalties into new industries. The ZTE penalty in March was the most obvious example of this trend, as it sent apowerful message to the worldwide community that US enforcers stand ready to impose massive punishments for the re-export of US-origin goods to Iran. The ZTE enforcement action is by far the largest of its kind, and the fact that it was mostly led by BIS and DOJ (not OFAC) suggests that the world business community now has to worry more about three powerful US enforcers in this area, not just two.

OFAC's penalty in June of 2017 against AIG was also significant. Though much smaller than the penalty against ZTE ('only' $150,000 USD), the OFAC announcement in conjunction with the AIG penalty signals that OFAC will be closely monitoring the insurance community's conduct with respect to countries subject to US sanctions. OFAC specifically criticised AIG both for entering into insurance contracts that did not exclude sanctioned countries, and also for what OFAC described as 'defective' exclusion clauses that did not sufficiently rule out providing insurance for shipments to sanctioned countries. This detailed level of criticism suggests that OFAC is closely monitoring the insurance industry and will likely continue to focus on that industry more generally.

Trend Three: Ever-expansive theories of US export controls and sanctions jurisdiction

Another trend to watch in 2018 is the ever-expansive theories of US export controls and sanctions jurisdiction. US enforcers already take a broad view of what conduct can give rise to US jurisdiction, applying US enforcement powers to all sales or resales of USorigin goods, even when conducted outside the US by entirely non-US parties. Likewise, the US takes the position that any involvement of the US financial system in a transaction, even if it involves nothing more than dollar

clearing in New York or replacement in the US of dollars that were, in the aggregate used in Iran transactions, triggers both civil and criminal jurisdiction over the entire transaction – including all foreign parties to the transaction – in the United States. These expansive theories of jurisdiction has been subject to criticism outside the United States, but two additional enforcement actions in 2017, suggest that US regulators' views of their extraterritorial powers are growing, not shrinking.

First, in an action involving a Taiwanese company, B Whale Corporation, OFAC found a violation of US law for a sale of Iranian oil in the Middle East to a non-US ship owned by B Whale because that ship had become a 'US person' under US law. How did this occur? It occurred because the Taiwanese company was before US bankruptcy courts at the time the sale occurred, and OFAC took the position that as a result, the ship was legally 'within the US' at the time of transaction. It remains to be seen whether this US person theory is unique to the facts of that case or whether it will be expanded.

Second, as noted briefly in a previous section, OFAC imposed a $12 million penalty imposed against two Singapore companies, CSE Global Limited and CSE TransTel Pte. Ltd., for using US dollars in connection with sales of non-US telecommunications equipment in Iran.

From OFAC's report on the enforcement action, it does not appear that any US person was involved in the dollar clearing of particular Iran transactions. Singapore banks conduct dollar clearing outside the United States and often have sufficient dollar reserves to do so. However, after dollar transactions have cleared, these banks replenish their reserves at the end of the day by obtaining more dollars from the US system. The transactions at issue in CSE appeared to fit this pattern; they were not cleared in the US, but the Singapore bank did utilise the US financial system to replace its dollar reserves (expended by processing any dollar transaction) at the end of the day. Even though no US person could be said to have 'serviced' any particular Iran transaction, OFAC took the position that CSE's use of dollar accounts in Singapore banks improperly 'caused' a US person to violate sanctions by providing a financial service to Iran. In doing so, OFAC relied on its position that CSE's use of dollars for these transactions violated CSE's agreements with its Singapore banks; it also suggests that the USD transfers intentionally omitted references to Iran. These enforcement actions continue to expand the limits of US enforcement jurisdiction. In 2018, expect US authorities to push these limits even further.

Trend Four: Enforcement of US sanctions against Russia expands

In 2014, the US and the EU imposed economic sanctions against Russia based on its conduct in the Ukraine. In the past few months, the US Congress has codified and potentially expanded those sanctions. But because the sanctions are so new, we have not had many signals about the vigour with which US enforcers will enforce them. Over the summer of 2017, OFAC imposed its first penalty under the sanctions, providing its first signal that US enforcers are going to move aggressively to enforce US sanctions against Russia. Look for the trend to continue in 2018.

Trend Five: Growing US enforcement actions involving China

China will also likely be a growing subject for US sanctions enforcement in 2018. During previous years, enforcement actions involving China have been relatively common with the most focus on the embargo of military sales to China and unlicensed sales of US-origin goods to Chinese entities on the US Commerce Department's Entity List. Nonetheless, enforcement of US sanctions and export controls in connection with shipments to China had not been on the scale of enforcement actions related to the Iran embargo or even the Syrian or Sudan embargoes.

But two things happened in 2017 to bring China more into play. First, the massive ZTE enforcement action put the spotlight on re-exports of US origin goods from China to countries subject to US embargo, in particular Iran. Expect that to continue in 2018, and potentially grow into a focus on sales from China in violation of the Russian sanctions.

Second, in September 2017, the US dramatically expanded sanctions against North Korea by significantly broadening secondary sanctions. Secondary sanctions target non-US persons for conduct outside the United States that is generally outside of the enforcement jurisdiction of US regulators. They are imposed through an order to the US financial system to avoid doing business with the target. As the US Secretary of the Treasury stated in September, foreign companies

targeted by secondary sanctions now must choose between access to the US financial system and doing business in North Korea. Since China, and particularly the Chinese financial system, reportedly has significant connections to the North Korean economy, it will be interesting to watch whether US regulators target the Chinese financial community with North Korean secondary sanction in 2018.

Indeed, already this year, the US Treasury has taken action against at least one Chinese bank based on its activities in North Korea. In June 2017, Treasury's Financial Crimes Enforcement Network ('FinCen') proposed to prohibit US financial institutions from opening or maintaining US correspondent accounts for Bank of Dandong, after having concluded that the Bank was acting 'as a conduit for illicit North Korean financial activity' and was a 'foreign financial institution of primary money laundering concern'. More recently, on 2 November 2017, FinCen published a final rule on this same subject that prohibits US financial institutions from opening or maintaining US correspondent accounts for Bank of Dandong, and also requires US financial institutions to apply special due diligence measures to their foreign correspondent accounts to guard against such accounts being used to process transactions involving Bank of Dandong. According to US regulators, 'restricting Bank of Dandong from accessing the US financial system – directly or indirectly – helps protect the US financial system from the illicit finance risks posed by Bank of Dandong and serves as an additional measure to prevent North Korea from accessing the US financial system.'

Trend Six: Continued focus on name and address screening practices

Another trend to watch in 2018 pertains to US enforcement focus on electronic name and address screening. Over the past few years, OFAC has imposed significant penalties against companies in the financial industry that have failed (in OFAC's view) to sufficiently screen transactions to ensure that individuals and entities on OFAC's SDN list are not able to conduct any transactions. As a practical matter, however, there are limits to how far this denial of access can go. If an SDN enters a fast-food restaurant and pays for a meal with cash, the fast-food company has theoretically violated US sanctions by making the sale, but such small commercial sales had been viewed as unlikely targets of enforcers.

Instead, it has been the expectation that such penalties would be targeted against the US financial system, placing the burden on the banking industry to generally deny access to persons and companies on OFAC's lists. This reflects not only the challenges of policing small transactions at the retail level, but also the considerable resources that systematic screening of such transactions requires. An electronic screening process requires companies to purchase and monitor software designed to identify SDNs, and it also requires a significant expenditure of human capital since ultimately compliance personnel must review any 'hit' in order to determine whether it constitutes an actual match to an entity on the SDN list. A recent OFAC enforcement action – against Richemont, the parent of the jeweller Cartier – suggests that these compliance burdens may extend well beyond the financial industry. In late September 2017, OFAC fined Richemont $334,000 for sending four shipments of jewellery to Shuen Wai Holding Limited in Hong Kong, which was on OFAC's SDN List.

The imposition of sanctions for retail sales of this sort could become a new trend, and could force all retailers to begin some sort of monitoring programme even for relatively small retail sales.

Trend Seven: Enforcement dangers posed by US persons, even where the underlying transaction appears to have little to no US connection

A final trend to watch in 2018 involves the enforcement dangers posed by US persons in multi-national transactions, even where the underlying transaction appears on the surface to have little or no US connection. This was a lesson learned most recently in an enforcement action brought against a US parent, White Birch Paper. On the surface, the penalised transactions appeared to involve only White Birch's Canadian subsidiary, which sent over half a million tons of Canadian-origin paper to Sudan pursuant to contacts between only the Canadian company and Sudanese customer. Had that been the entirety of the transaction, it would have been completely lawful. However, a penalty against the US parent was imposed after OFAC determined that personnel from the US parent were involved in 'discussing, arranging, and executing the export transactions to Sudan…' a violation of US sanctions had occurred. There were other features of the conduct that

were in play as well, especially the Canadian subsidiary's alteration of financial documents to prevent banks from knowing the intended destination of the paper.

A similar blurring of the line between US parent and foreign subsidiary also occurred when OFAC imposed a $259,200 civil penalty against IPSA International Services, whose Canadian and Dubai subsidiaries obtained due diligence services in Iran but the US parent 'facilitated the foreign subsidiaries' engagement in such transactions because IPSA reviewed, approved, and initiated the foreign subsidiaries' payments to providers of Iranian-origin services.'

This trend reinforces the advice that is often provided to foreign multinational companies seeking to do lawful business in jurisdictions that are under US embargo. Such transactions may be legal on their face, but extreme diligence is needed to ensure that they do not run afoul of US law by including US persons (entities or individuals) or the US financial system at some point in the chain. That risk is very hard to manage, and will likely continue to be so going forward.

Originally published in the December 2017 issue of WorldECR.