Compliance lessons in recent Office of Foreign Assets Control enforcement

Received (in revised form) 3rd November, 2020

Ben Hutten
Counsel, Buckley, USA

Ben Hutten

Benjamin W. Hutten *is Counsel at Buckley LLP. He provides regulatory and compliance counsel, as well as internal investigative and enforcement defense services, to foreign and domestic financial institutions. He has represented numerous foreign financial institutions in cross-border, multiagency criminal and regulatory investigations into past compliance with US sanctions and anti-money laundering (AML) laws and regularly provides representation in front of the Office of Foreign Assets Control (OFAC). Benjamin has a deep understanding of sanctions and AML regulations and enforcement. In addition to his client work, he has participated in numerous financial industry group regulatory initiatives related to sanctions and AML issues, including The Clearing House Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking, initiatives to address 'de-risking', and initiatives related to AML-related information sharing. Benjamin also conducts international trainings in AML and sanctions issues for the Financial Services Volunteer Corps. Buckley LLP offers premier government enforcement, litigation, compliance, regulatory and transactional services to US and international financial institutions, corporates and individuals, with a core strength in financial services.*

Abstract

In May 2019, the US Department of the Treasury's Office of Foreign Assets Control (OFAC), which administers US sanctions laws, issued a broad framework identifying what OFAC views as the essential elements of risk-based sanctions compliance. At the same time, OFAC announced that it would consider how well these elements have been incorporated when considering its enforcement response to sanctions violations. While providing general guidance, the framework provides little in the way of practical detail to assist financial institutions with incorporating the framework into their organisations. Perhaps in recognition, OFAC recommended that all organisations review enforcement actions published by OFAC for purposes of reassessing and enhancing sanctions compliance. This paper is intended to help financial institutions comply with OFAC's recommendation by identifying critical guidance and common pitfalls in a survey of post-framework enforcement actions.

Keywords: OFAC, sanctions, screening, diligence, risk assessment, enforcement, training, sanctions evasion, false hits

Buckley LLP,
1133 Avenue of the Americas,
Suite 3100, New York,
NY 10036,
USA
Tel: +1 212 600 2333;
E-mail: bhutten@buckleyfirm.com

Journal of Financial Compliance
Vol. 4, No. 3 2021, pp. 210–221

2398-8053

INTRODUCTION

In May 2019, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued its Framework for Compliance Commitments (the 'Framework'), which, for the first time, outlined OFAC's views on essential elements of a risk-based sanctions compliance programme (SCP). OFAC indicated that in future enforcement actions, it would determine whether elements of the Framework should be incorporated into the SCP of the party subject to enforcement and whether it would require compliance commitments as a condition of settlement. OFAC also recommended that 'organizations subject to US jurisdiction' assess its future enforcement actions and enhance their SCPs whenever they found gaps against expectations articulated in the actions.[1]

This paper analyses the compliance programme guidance OFAC has set out in

public enforcement actions taken since issuing the Framework. It highlights common themes and pitfalls and discusses how financial institutions can implement lessons from the actions. US financial institutions — all of which must comply with OFAC requirements — and particularly those conducting international business are likely to be interested in the discussion. It should also be of interest to foreign financial institutions conducting international business that, however remotely, has a connection to the United States that could make them subject to OFAC's requirements and enforcement authority. A chart featuring post-Framework enforcement highlights and pitfalls is included at the end of this paper.

OVERVIEW OF POST-FRAMEWORK ENFORCEMENT ACTIVITIES

Since issuing its Framework, OFAC has issued 26 public enforcement actions, which is significantly higher than the previous few years.[2] Of these, 5 were findings of violations, and 21 were civil money penalties. Eight involved financial institutions, 17 involved nonfinancial companies, and 1 involved an individual.[3] The smaller proportion of actions against financial institutions should not lead financial institutions into a sense of complacency. The number of actions involving financial institutions is generally consistent with past years, but the elevated number of enforcement actions against nonfinancial companies is reflective of OFAC's increasing focus on that group. The largest penalty, by far, was against a non-US bank and would have been much higher but for OFAC's determination that the bank would face a disproportionate impact if it were required to pay the originally proposed settlement amount.[4] OFAC's largest penalties have historically been imposed on financial institutions, which reflects OFAC's enhanced compliance expectations on financial institutions, which serve as gateways to — and have been deputised by the US government as guardians of — the US financial system.

In conjunction with the Framework, OFAC listed ten common pitfalls, referred to as 'root causes' of sanctions violations and compliance programme breakdowns.[5] Examples of these pitfalls abound in post-Framework actions. The actions discussed here, however, put a finer point on ways in which the pitfalls arise, contain new ones and, importantly, contain guidance about how OFAC expects them to be prevented. Overall, post-Framework actions demonstrate that OFAC maintains high expectations regarding the capabilities and sophistication of OFAC compliance programmes, which in turn puts pressure on institutions to modify compliance measures accordingly. Perhaps the most important and detailed guidance from post-Framework actions is in the area of screening. OFAC has previously made clear that it expects companies engaged in international business to use screening software with sophisticated capabilities, and its enforcement actions since issuing the Framework provide a wealth of detail on what those capabilities should be. Also important are expectations articulated by OFAC about initial and continuing customer due diligence, including diligence regarding customers' customers and counterparties, as well as expectations about being able to identify weaknesses in sanctions controls and warning signs of sanctions evasion. The most significant lessons and guidance from OFAC's post-Framework enforcement actions are summarised here.

UNSOPHISTICATED SCREENING IS A PROBLEM

OFAC's post-Framework actions contain a wealth of information about its expectations in the area of screening capabilities. This information is important, as screening

of customer, counterparty and transactional data is one of the primary ways that institutions identify and interdict prohibitive business with sanctions targets. As OFAC indicated, software that detects only exact matches is likely insufficient for all but lowest-risk activities. Instead, screening software should be able to detect common alternative spellings of sanctioned countries or parties, such as 'Kuba' instead of 'Cuba'. OFAC's settlement with Amazon, in which Amazon failed to detect the word 'Krimea' as a common variant of the sanctioned jurisdiction of Crimea, reiterated this point.[6] Similarly, in its settlement with Deutsche Bank Trust Company Americas, OFAC faulted Deutsche Bank for calibrating its screening to detect only exact matches.[7]

In addition, OFAC's post-Framework actions put a finer point on OFAC's expectations about filter capabilities, making clear that for international businesses, it expects screening to be sophisticated in the ways described here. Financial institutions conducting international business may wish to carefully consider whether their screening solutions have these capabilities.

- **Screen for Cities and Ports in Embargoed Jurisdictions.** For businesses that operate on a global scale, screening should include the names and common alternative spellings of major cities and ports within jurisdictions subject to broad-based sanctions. For example, OFAC highlighted Amazon's failure to detect an address in 'Yalta', a well-known Crimean port city.[8]
- **Identify and Screen for Full and Abbreviated Names.** In its settlement with General Electric (GE), OFAC faulted GE for ineffective screening. In that case, GE was presented with checks containing the full name of a Specially Designated Nationals (SDN). GE's screening software, however, utilised only a common abbreviation of the SDN's name and, thus, did not detect the match.[9] OFAC's characterisation of GE's screening capabilities as ineffective suggests that it expects screening to be able to identify both full names and common abbreviations.
- **Recognise Variations and Punctuation in Common Corporate Suffixes.** Legal entities' use of capitalisation and punctuation in common corporate suffixes varies widely. For entities operating on a global scale, OFAC expects filtering software to have the capability to account for these variations. For example, OFAC noted in its settlement with Apple that Apple did not detect that its client — listed in Apple's records as 'SIS DOO' — was a match to the SDN 'SIS d.o.o'. The term 'd.o.o' is a common corporate suffix in Slovenia. OFAC faulted Apple for failing to detect the match for over two years.[10]
- **Screen Addresses and Location Data.** In addition to identifying persons located in sanctioned jurisdictions, address screening provides additional data points for use in detecting matches to information on OFAC's lists. In the preceding example regarding SIS d.o.o., the customer's address in Apple's records exactly matched the address in OFAC's List of Specially Designation Nationals and Blocked Persons (the 'SDN List'). Screening of address information could have provided an additional safeguard, even if the variation in capitalisation and punctuation caused filtering software not to flag the client's name. In OFAC's words, '[c]ompanies should consider OFAC screening and compliance measures that exploit names, addresses, and other identifying information on the SDN List'.[11]
- **Screen Appropriate Third Parties.** One of the most fundamental decisions in developing an SCP is determining which data should be screened, including which customer-associated parties and third parties to screen. These decisions

should include an assessment of whether screening of any particular party or data would indicate some sort of connection between the customer and a sanctioned person or jurisdiction. For example, in the Apple action, OFAC noted that SIS d.o.o.'s director and majority owner was also an SDN. Apple's records at the time listed the owner as an 'account administrator' a data point that was — at the time — not screened. OFAC characterised this as a 'point of failure'.[12]

- **Ensure Data Is Stored Correctly.** An action against Western Union highlights the importance of storing and characterising data in way that ensures sanctions-relevant data is fed into screening software. In that action, a foreign bank was one of Western Union's master agents in The Gambia. The bank then established a sub-agent relationship with the Kairaba Shopping Center, an entity that was subsequently designated by OFAC under its Global Terrorism Sanctions Regulations. Although Western Union had a process to screen sub-agents, Western Union characterised the Kairaba Shopping Center in its records as a location of the bank, instead of a separate sub-agent. Because, at the time, Western Union did not screen location data, it did not identify Kairaba Shopping Center as an SDN until years after its designation.[13]

DUE DILIGENCE EXTENDS TO KNOWING CUSTOMERS' CUSTOMERS AND COUNTERPARTIES

OFAC's Framework makes clear that it expects persons subject to US jurisdiction to conduct sanctions-related customer due diligence that is commensurate with risks posed by the relationship or transaction. Post-Framework enforcement actions make clear that this diligence should be ongoing and should include a general understanding of the customers' customers and counterparties and, in some instances, identifying and assessing risks associated with individual customer or counterparties of the customer.

The GE action highlights that in high-risk situations, OFAC could expect an entity to know its customer's customers and counterparties. From 2010 to 2014, three GE subsidiaries accepted payment on 289 occasions from The Cobalt Refinery Company, an SDN, for goods and services provided to a Canadian customer of GE. According to OFAC, publicly available information demonstrated that the Canadian customer had ties to the Cuban mining industry through joint ventures with the Cuban government and that Cobalt was owned by a joint venture between the Canadian customer and the Cuban government. OFAC faulted GE for failing to 'take reasonable care' with respect to US sanctions obligations, indicating that it expected GE's diligence to identify both that the Canadian customer was involved in business with the Cuban government and that its counterparties were government owned.[14]

DUE DILIGENCE SHOULD BE ONGOING

The GE action also highlights the importance of conducting ongoing due diligence. Notwithstanding the publicly available information about the Canadian customer, the GE subsidiaries renewed the customer relationship on at least 18 occasions. In OFAC's words, the GE action 'demonstrates the importance of conducting appropriate due diligence on customers and other counter-parties when *initiating* and *renewing* customer relationships'.[15] Thus, if a transaction or relationship is renewable, financial institutions should consider reassessing associated OFAC risks. As demonstrated by the GE action, periodic reassessments become more important as risk increases.

IDENTIFY SYSTEM WEAKNESSES AND AVENUES OF SANCTIONS EVASION

OFAC's actions against Apple and American Express Travel Company demonstrate its expectation that institutions anticipate and identify control weaknesses as potential avenues of sanctions evasion. For example, in the Apple action, OFAC explicitly stated that sanctions compliance programmes should include preventative measures that alert and react to sanctions evasion warning signs, such as business and employment connections between sanctions-targeted individuals and entities.[16]

OFAC's guidance was in response to Apple's transfer of a portion SIS d.o.o.'s applications sold in the App Store to a second software company that was incorporated several days after the designation of SIS d.o.o, and the transfer of the remainder of SIS d.o.o.'s applications to a third company that took over the administration of SIS d.o.o.'s App Store account, all without personnel oversight or screening by Apple.[17] In the action against American Express Travel Company, an SDN applied for a prepaid travel card through a non-US bank, which at the time was an authorised issuer of the travel card. The sanctions screening system used at the time generated multiple declined messages to the non-US bank, which continued to make several additional approval attempts. The continued attempts led the screening tool to 'time out', which triggered the application to be automatically approved. OFAC noted that 'this case highlights the importance of taking the steps necessary to ensure that automated sanctions compliance controls measures cannot be overridden without appropriate review'.[18] Building in additional layers of review as well as identifying potential control weaknesses during the OFAC risk assessment — which generally assesses the quality of controls in light of risk — can help identify potential weaknesses and avenues of exploitation by sanctions evaders.

US CONNECTIONS CAN ARISE IN UNEXPECTED WAYS

Generally, non-US financial institutions are required to comply with OFAC's requirements only when conducting business that has some connection to the United States. Post-Framework enforcement actions highlight a number of instances where a US connection arose in ways not previously asserted by OFAC.

The first is the provision of US-origin goods that benefits sanctions targets, even if the transaction is conducted outside the United States and the applicable sanctions laws do not purport to prohibit re-exportation of US-origin goods form a third country. This type of connection arose in the action against Société Internationale de Télécommunications Aéronautiques SCRL (SITA), which is headquartered in Switzerland and provides commercial telecommunications network and information technology services to the civilian air transportation industry. At issue were services provided to airlines designated under OFAC's Global Terrorism Sanctions Regulations. SITA provided the airlines with access to a software application of US origin that allows shared users of a common terminal to manage check-in and baggage transportation. Apart from its origin, OFAC did not allege that the software was hosted on US servers or was otherwise connected to the United States at the time of its use. The sole US connection articulated by OFAC was the provision of US-origin software knowing its use would benefit the designated customers.[19] The action raises questions about why OFAC concluded that it had jurisdiction over this activity, because the Global Terrorism Sanctions Regulations do not prohibit the re-export of US-origin goods to sanctions targets, and also raises unanswered questions about whether foreign financial institutions and corporates need to ensure that any US-origin software

they use is not made available for benefit of targets of the Global Terrorism Sanctions Regulations and similar regimes.[20]

Additionally, OFAC's action against British Arab Commercial Bank (BACB) highlights novel risks related to offshore banking arrangements in US dollars. Because the facts of the case are important, they are replicated from OFAC's enforcement release here:

> BACB established a USD [US dollar] nostro account in 2006 with a non-US financial institution located in a country that imports Sudanese-origin oil for the stated purpose of facilitating payments involving Sudan. BACB funded this nostro account by routing large, periodic, USD-denominated wire transfers into the account (ie bulk funding) from non-US financial institutions in Europe. The non-US financial institutions in Europe then passed the USD-denominated transfers through banks in the United States for further credit to the USD nostro at the non-US financial institution. Once the funds arrived in BACB's USD nostro at this institution, BACB instructed the institution to process individual payments (ie third-party payments) involving a variety of Sudanese parties, including Sudanese financial institutions. OFAC's analysis of the transactional data confirmed a pattern of the bulk funding transactions, which were processed through the United States, corresponding to the third-party payments, which were not processed through the United States.[21]

The upshot is that even if US dollar transactions with sanctions targets occur wholly outside the United States, there may be some risk of OFAC asserting jurisdiction if the dollars used to fund that transaction previously passed through the United States. Because all US dollars at some point originate in the United States, the BACB case leaves foreign institutions with very little guidance as to when the connection between US dollars and the United States becomes too attenuated for US jurisdiction to arise. Perhaps the best clue comes from OFAC's assertion that its 'analysis of the [BACB] transactional data confirmed a pattern of the bulk funding transactions, which were processed through the United States, corresponding to the third-party payments [involving sanctions targets]'.[22] This language suggests that, unlike traditional bulk funding payments, the payments that passed through the United States were made primarily to fund BACB's offshore US dollar transactions with sanctions targets. Thus, non-US financial institutions that conduct offshore transactions with sanctions targets in US dollars should closely review funding mechanisms involving the United States, and identify how closely payments cleared through the US financial system correspond to offshore transactions involving sanctions targets.

AVOID MISUNDERSTANDINGS BY SEEKING EXPERT ADVICE ABOUT SANCTIONED PARTY INVOLVEMENT

As OFAC pointed out in the Framework, misunderstanding and lack of awareness of sanctions requirements are common pitfalls for both US and non-US companies. Post-Framework enforcement actions highlight the dangers of two common types of misunderstanding: misunderstanding the scope of general licenses authorising certain activities with sanctions targets, and creating complex structures in an effort to avoid violating sanctions requirements.

Enforcement actions against Atradius Trade Credit Insurance, Inc., Park Strategies LLC, and Aero Sky Aircraft Maintenance, Inc., illustrate the dangers of misunderstanding the scope of a general license authorising transactions with a

sanctions target. In the Atradius action, a US cosmetics company assigned Atradius, a US trade credit insurer, approximately US$5m in debt owned by a Panamanian SDN. Misunderstanding the scope of a general license permitting the liquidation of the SDN's assets, Atradius filed a claim in Panama as a creditor of the SDN and received payment on that claim in violation of the OFAC's sanctions on foreign narcotics kingpins. Among other things, OFAC faulted Atradius for not undertaking any meaningful analysis of — or seeking advice from OFAC regarding — whether its activities were permissible under existing authorisations.[23] Similarly, in its action against Park Strategies, a US corporate lobbying group, OFAC indicated that the firm provided lobbying services to the SDN as a result of misunderstanding the scope of a general license that permits the provision of legal services.[24] In the Aero Sky action, an airline service provider entered into a contract with an airline designated under OFAC's global terrorism sanctions on the mistaken belief that a general license related to the Iranian civil aviation industry permitted this activity.[25]

These three actions demonstrate that it is particularly important to have experts carefully analyse the scope of any general license relied upon to conduct business with a sanctions target. By design, general licenses are intended to permit only very limited transactions with sanctions targets that are otherwise deemed dangerous to US interests. Licenses are often subject to numerous conditions, limitations and reporting requirements. Thus, as OFAC noted in the Aero Sky action, persons dealing with sanctions targets under a general license 'should ensure they carefully review, and fully comply with, all of the terms and conditions of those licenses'.[26]

Two other actions, against Hotelbeds USA, Inc., and Biomin America, Inc., illustrate a separate point, but one that continues to recur: creating complex arrangements to enable the conducting of business that might otherwise be prohibited is risky at best. Doing so without appropriate review and expert advice is a bad idea because the structures are often based on a misunderstanding of sanctions laws. Hotelbeds USA is a US subsidiary of Hotelbeds Group, headquartered in Spain. On the mistaken belief that it would render Cuba-related activity permissible, Hotelbeds USA set up a structure in which it sold hotel accommodations in Cuba, directed payment to an account in Spain and then was subsequently credited for revenues from these payments. This misunderstanding may have arisen because 'Hotelbeds USA had only an informal compliance program' that was 'incommensurate with risks associated with providing international travel services'.[27] Similarly, Biomin America, a US animal nutrition company, developed a structure in which Biomin America processed purchase orders from a Cuban company on behalf of Biomin's foreign affiliates that would then fulfill the orders for the Cuban company. Again, this was done on the mistaken belief that the structure complied with US sanctions requirements, because the company 'failed to seek appropriate advice or otherwise take the steps necessary to authorize these transactions'.[28]

The five actions discussed previously also illustrate the importance of escalating sanctions-connected transactions to internal or external resources with appropriate expertise — which likely would have prevented the conduct at fault. It is, therefore, advisable to maintain documented procedures that require escalation of activities in which a sanctioned party or jurisdiction is involved to experts. Additionally, it is advisable to conduct sufficient training to enable personnel to recognise situations in which escalation

is necessary and understand escalation channels.

TRAIN, AUDIT AND MONITOR NON-US SUBSIDIARIES OF US PARENTS

US sanctions programmes that require compliance by foreign subsidiaries of US persons pose unique risks and continue to confound in post-Framework enforcement actions. For this reason, US parent companies should train, audit and monitor foreign subsidiaries for sanctions compliance.

Generally, compliance with OFAC-administered sanctions is required only for US persons or for transactions by non-US persons that have a US nexus. For nearly all sanctions programmes, a US person means 'any United States citizen or national; permanent resident alien; entity organised under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States'.[29] Thus, foreign-incorporated subsidiaries of US companies are generally not required to comply, absent a connection between the United States and the business conducted. There are exceptions, however, that frequently cause compliance headaches. OFAC's sanctions on Cuba are frequently to blame, because they require compliance at all times by both US-incorporated entities and their foreign subsidiaries.[30] Similarly, foreign subsidiaries of US parent companies are subject to numerous provisions of the Iranian Transactions and Sanctions Regulations.[31] Most recently, OFAC amended the North Korea Sanctions Regulations to apply to non-US entities owned controlled by US financial institutions.[32]

Activities of foreign subsidiaries pose higher risks because the non-US persons with which they deal in their home countries are not subject to the same restrictions on dealing with sanctions targets. This risk is especially high where a US company acquires a foreign subsidiary not previously owned or controlled by a US person and was free to deal with US sanctions targets. For example, in the action against Expedia Group, Inc., a US company, Expedia and its subsidiaries assisted over 2000 persons with Cuba-related travel services. According to OFAC, the violations occurred because Expedia acquired 'foreign subsidiaries [that] lacked an understanding of and familiarity with US economic sanctions laws and Expedia employees overlooked particular aspects of Expedia's business that presented risks of noncompliance with sanctions . . . [w]ith respect to at least one foreign subsidiary, Expedia failed to inform the subsidiary until approximately 15 months after Expedia acquired the subsidiary that it was subject to US jurisdiction and law'.[33] As noted by OFAC, this case highlights the importance of 'conducting sanctions-related due diligence both prior and subsequent to mergers and acquisitions, and taking appropriate steps to audit, monitor, train, and verify newly acquired subsidiaries for OFAC compliance'.[34]

Similar examples abound in post-Framework actions, even outside the context of acquisitions. US-based company PACCAR had a wholly owned subsidiary in Germany that sold or supplied trucks to customers in Europe that it knew or had reason to know were ultimately intended for customers in Iran. OFAC noted that its action against PACCAR 'highlights the benefits US companies can realize in conducting sanctions-related training and in taking appropriate steps to audit and monitor foreign subsidiaries for OFAC compliance. US parent companies can mitigate risk to sanctions exposure by proactively establishing and enforcing a robust sanctions compliance program'.[35] Thus, it is advisable for US parent companies to pay close attention to sanctions compliance of their non-US subsidiaries.

CAREFULLY MANAGE 'GOOD GUY' OR 'FALSE HIT' LISTS

OFAC's action against American Express highlights another common compliance pitfall: the 'good guy' or 'false hit' list. These lists are meant to reduce unnecessary time spent reviewing alerts. They do so by suppressing future alerts generated by sanctions screening software on customers or counterparties that have previously been evaluated and deemed compliant. Without careful management, however, they pose two significant risks. First, if a sanctions target is wrongly added to the good guy list, the institution will continue to conduct potentially violative business without being alerted. Secondly, OFAC's sanctions change frequently, which can have a significant impact on good guy lists.

The American Express action illustrates the point. As noted previously, a system 'time out' due to repeated attempts to apply for a prepaid card caused the application of an SDN to be automatically approved. After the approval was generated, the screening software automatically routed the application into a queue for manual review of potential sanctions issues. The compliance analyst that reviewed the alert incorrectly determined the match to be a false positive and added the applicant to the 'Accept List'. As a result, the SDN was able to engage in multiple future card loads and withdrawals in violation of OFAC sanctions.[36]

As this action illustrates, it is important to build in multiple levels of review by appropriately experienced sanctions personnel when adding to good guy lists. It is also important to frequently review the list for purposes of determining if changes in sanctions require modifications. Finally, it is important to ensure that meaningful changes to customer information trigger a review of the customer's entry on the list.[37]

As demonstrated previously, OFAC enforcement contains a wealth of guidance that puts a finer point on the compliance expectations articulated in OFAC's Framework. To the extent that an institution's business or customers are substantially similar to those in the enforcement actions discussed previously, the institution should consider looking more closely at the action itself for further guidance as well as reviewing its own SCP for purposes of avoiding similar pitfalls.

References

(1) OFAC, 'A framework for OFAC compliance commitments' (2nd May, 2019), available at: framework_ofac_cc.pdf (treasury.gov) (accessed 25th November, 2020). The Framework listed five essential elements of a SCP: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing, and (5) training.

(2) OFAC issued 7 enforcement actions in 2018, 16 in 2017 and 9 in 2016.

(3) This count is as of 10th September, 2020. The civil money penalty against the individual is not considered in this paper because it does not discuss issues facing financial institutions.

(4) *See* OFAC, 'Settlement agreement with British Arab Commercial Bank' (3rd September, 2019). OFAC assessed a US$4m penalty in light of the proposed US$228m penalty amount.

(5) OFAC, ref. 1 above.

(6) OFAC, Enforcement Release, 'OFAC settles with Amazon.com, Inc. with respect to potential civil liability for apparent violations of multiple sanctions programs' (8th July, 2019), available at: 20200708_amazon.pdf (treasury.gov) (accessed 25th November, 2020).

(7) OFAC, Enforcement Release, 'OFAC Enters $583,100 Settlement with Deutsche Bank Trust Company Americas for Apparent Violations of Ukraine-Related Sanctions Regulations and Executive Order 13685 of December 19, 2014', 'Blocking property of certain persons and prohibiting certain transactions with respect to the Crimea region of Ukraine' (9th September, 2020).

(8) *Ibid*.

(9) OFAC, Enforcement Release, 'The General Electric Company settles potential civil liability for alleged violations of the Cuban Assets Control Regulations' (1st October, 2019), available at: 20191001_ge.pdf (treasury.gov) (accessed 25th November, 2020).

(10) OFAC, Enforcement Release, 'Apple, Inc. settles potential civil liability for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations' (25th November, 2019), available at: 20191125_apple.pdf (treasury.gov) (accessed 25th November, 2020).

(11) *Ibid*.

(12) *Ibid*.
(13) OFAC, Enforcement Release, 'Western Union Financial Services, Inc. settles potential civil liability for apparent violations of the Global Terrorism Sanctions Regulations' (7th June, 2019), available at: 20190607_western_union.pdf (treasury.gov) (accessed 25th November, 2020).
(14) OFAC, ref. 9 above.
(15) *Ibid* (emphasis in original).
(16) OFAC, ref. 10 above.
(17) *Ibid*.
(18) OFAC, Enforcement Release, 'OFAC issues a finding of violation to American Express travel related services company for violations of the weapons of Mass Destruction Proliferators Sanctions Regulations', (30th April, 2020), available at: 20200430_amex.pdf (treasury.gov) (accessed 25th November, 2020).
(19) OFAC, Enforcement Release, 'Société Internationale de Télécommunications Aéronautiques SCRL ("SITA") settles potential civil liability for apparent violations of the Global Terrorism Sanctions Regulations' (26th February, 2020), available at: 20200226_sita.pdf (treasury.gov) (accessed 25th November, 2020).
(20) The SITA action also highlights another often-overlooked connection to the United States: technology and infrastructure that is based in the United States. OFAC also faulted SITA for providing messaging services to the designated airlines that were routed through switches in the United States and global lost baggage services, the data for which was hosted on a US server. This highlights the need for non-US institutions to carefully consider whether US-based technology and/or servers are involved in any of their dealings with sanctions targets and the need for such technology or servers to be firewalled from sanctions-facing business. *Ibid*.
(21) OFAC, ref. 4 above.
(22) *Ibid*.
(23) OFAC, Enforcement Release, 'Atradius Trade Credit Insurance, Inc. settles potential liability for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations' (16th August, 2019), available at: 20190816_atci.pdf (treasury.gov) (accessed 25th November, 2020). While OFAC faulted Atradius for not seeking counsel from OFAC, it should be noted that, if done incorrectly, contacting OFAC can itself carry risks such as business delays or investigations and should be done carefully only after consultation with in-house or external experts.
(24) OFAC, Enforcement Release, 'Park Strategies, LLC settles potential civil liability for apparent violations of the Global Terrorism Sanctions Regulations' (21st January, 2020), available at: 20200121_park_strategies.pdf (treasury.gov) (accessed 25th November, 2020).
(25) OFAC, Enforcement Release, "OFAC issues a finding of violation to Aero Sky Aircraft Maintenance, Inc. for violations of the Global Terrorism Sanctions Regulations' (12th December, 2019), available at: 20191212_aero_sky.pdf (treasury.gov) (accessed 25th November, 2020).
(26) *Ibid*.
(27) OFAC, Enforcement Release, 'Hotelbeds USA, Inc. settles potential civil liability for apparent violations of the Cuba Assets Control Regulations' (13th June, 2020), available at: 20190612_expedia.pdf (treasury.gov) (accessed 25th November, 2020).
(28) OFAC, Enforcement Release, 'OFAC settles with BIOMIN America, Inc. with respect to potential civil liability for apparent violations of the Cuban Assets Control Regulations' (6th May, 2020), available at: 20200506_biomin.pdf (treasury.gov) (accessed 25th November, 2020). Additionally, OFAC highlighted the risk of using complex payment structures in the British Arab Commercial Bank action. *See* OFAC, ref. 4 above.
(29) *See*, *eg,* 31 CFR § 560.314.
(30) *See* 31 CFR § 515.329.
(31) For purposes of OFAC's Iran sanctions, foreign subsidiaries of US persons are prohibited from 'knowingly' engaging in most transactions involving Iran, even where the transactions have no US nexus. 31 CFR § 560.215.
(32) 31 CFR § 510.214.
(33) OFAC, Enforcement Release, 'Expedia Group, Inc. ("Expedia") settles potential civil liability for apparent violations of the Cuban Assets Control Regulations' (3rd June, 2019), available at: 20190612_expedia.pdf (treasury.gov) (accessed 25th November, 2020).
(34) *Ibid*.
(35) OFAC, Enforcement Release, 'PACCAR Inc. settles potential civil liability for apparent violations of the Iranian Transactions and Sanctions Regulations' (6th August, 2019), available at: 20190806_paccar.pdf (treasury.gov) (accessed 25th November, 2020).
(36) OFAC, ref. 18 above.
(37) For further guidance, see OFAC, 'False hit list guidance' (21st October, 2015), available at: false_hit.pdf (treasury.gov) (accessed 25th November, 2020).

Annex 1: Summary Table of Post-Framework Enforcement

Category of Guidance	*Summary of Post-Framework Enforcement Guidance*	*Relevant Action*	*Takeaway*
Screening capabilities	• Screening only for exact matches is often insufficient • Screen for major cities and ports in embargoed jurisdictions • Recognise variations and punctuation in corporate suffixes • Screen address/location data • Screen appropriate third parties • Ensure data is correctly fed to screening tool	• Amazon • GE • Apple • Western Union	Financial institutions conducting international business may wish to carefully consider whether their screening solutions have the capabilities highlighted by OFAC.
Due diligence	• OFAC diligence should be ongoing • Diligence should include a general understanding of a customer's customers and counterparties • In high-risk situations, OFAC may expect diligence into individual customers or counterparties of the customer	• GE	Financial institutions may wish to ensure that types of customers and counterparties of their customers are known, and that publicly available information about significant business by the customer with sanctions targets is evaluated
Identifying weaknesses/evasion	• Compliance programmes should have preventative measures to alert and evaluate evasion warning signs • Automated controls should not be overridden without review	• Apple • Western Union	Financial institutions should evaluate their sanctions compliance programmes for weaknesses and ways in which controls could be evaded and remediate accordingly
Application of sanctions to foreign persons	• US jurisdiction (and OFAC compliance requirements) can arise in unexpected ways, and OFAC may assert jurisdiction over tenuous US connections	• SITA • BACB	Foreign financial institutions should carefully and broadly identify business connections to the United States, as well as potential connections to sanctions targets, as part of their sanctions risk assessment
Understanding of OFAC require-ments	• The scope, terms and conditions of general licenses must be carefully evaluated • Creating complex structures to enable business that would otherwise be prohibited is risky at best	• Atradius Credit Insurance • Park Strategies • Aero Sky Aircraft Maintenance • Hotelbeds USA • Biomin America	Financial institutions should ensure experts carefully review business with sanctions targets conducted under general licenses or complex structures
Affiliate oversight	• US sanctions programmes on Cuba and Iran, which require compliance by foreign subsidiaries of US persons, pose unique risks	• Expedia • PACCAR	US persons merging with or acquiring a foreign business should conduct careful sanctions due diligence prior to and after the transaction. US persons should also train, audit and monitor foreign subsidiaries in the area of OFAC compliance

(*Continued*)

Annex 1: Summary Table of Post-Framework Enforcement (*Continued*)

Category of Guidance	*Summary of Post-Framework Enforcement Guidance*	*Relevant Action*	*Takeaway*
Good guy/false hit lists	• False hit/good guy lists pose significant risks if a sanctions target is wrongly added or if the list is not revised to address changes to sanctions requirements	• American Express	Financial institutions should include multiple levels of review by appropriately trained person when adding to the good guy list, and frequently review the list in light of changing OFAC requirements

Notes: BACB, British Arab Commercial Bank; GE, General Electric; OFAC, Office of Foreign Assets Control; SITA, Société Internationale de Télécommunications Aéronautiques SCRL.