Navigating the Complex Landscape of Economic Sanctions: Challenges, Best Practices, and Recent Enforcement Actions

Author: David Kearney, MLRO, AIB Merchant Services with the support of the Compliance Institute's Financial Crime Compliance Working Group.

Introduction

The Financial Crime Compliance Working Group published an article on sanctions compliance in the autumn edition of the ICQ in 2020. That article discussed the essential components of a risk-based sanctions framework and the regulatory expectations around each component, the various competent authorities that compliance professionals might encounter, and the effects of Brexit on the UK sanctions regime.

At the time, most compliance professionals did not have much exposure to sanctioned entities, sanctioned individuals, or prohibited/dual use goods. The Russian invasion of Ukraine on the 24th of February 2022, and the subsequent reaction by western powers has brought sanctions compliance to the forefront for all firms.

As stated in the 2020 article, financial sanctions can be defined broadly as an economic (as opposed to diplomatic or military) measure taken by one country or group of countries to alter the strategic decisions of another country, organisation or individual, and/or to induce that country, organisation or individual to change some policy or practices. This was certainly the case in relation to the western response to the invasion. Sanctions were imposed on prominent Russian businesspeople living inside and outside of Russia, Russian banks and their European subsidiaries were sanctioned, and in a further measure, bans were placed on the export of certain goods to Russia.
Against the backdrop of an ever-evolving sanctions environment, the impact of global sanctions regimes on firms and compliance processionals is ever-present, as the United States, the European Union and the United Kingdom continue to designate additional entities and individuals under various sanctions programs.
On 2nd of November 2023, the Office of Foreign Asset Control (OFAC) designated 130 entities and individuals as sanctioned under the US-Russian related sanctions regime; the list of 130 also included two Irish nationals.

This article discusses the evolving landscape of global sanctions compliance, particularly in the aftermath of the Russian invasion of Ukraine in February 2022. Delving into the essential components of a risk-based sanctions framework, the discussion revolves around the nuanced interpretation of the 50% rule across the European Union, the United States, and the United Kingdom. The article further explores key enforcement actions, emphasizing the importance of due diligence in funding accounts, the timing of sanctions reviews, and the significance of geo-location and IP address checks. It concludes by highlighting the imperative for robust employee training and a proactive approach to navigate the complexities of sanctions compliance in an ever-changing geopolitical environment.

The 50% Rule

In order for a legal person to be sanctioned, it must be owned or controlled by a sanctioned individual or another sanctioned entity, but what does "owned" or "controlled" mean in practical terms?

In April 2023, the European Union hosted an event focused on sanctions that featured a presentation by an expert from the Council of Europe. The presentation highlighted good practices as well as the challenges faced in implementing EU international sanctions. The presenter also discussed the definitions of ownership and control:

Ownership: The determination of whether a legal entity is owned by another entity involves considering possession of over 50% of proprietary rights or holding a majority interest. If these conditions are met, the legal entity is regarded as being owned by the other entity.

Control: When evaluating whether a legal entity is under the control of another individual or entity, either independently or as per an agreement with another

shareholder or a third party, various factors, including different methods of influence and the exercise of powers, may be considered.

The European Union, the United States and the United Kingdom all have different versions of the 50% rule when determining whether a legal person is owned or controlled by a sanctioned individual or entity:

EU Sanctions Obligations

- Compliance professionals in firms subject to the European Union sanctions regime should look at the aggregated ownership of the legal person. If one sanctioned individual owns 30% of the legal person, and one sanctioned individual owns 21% of the legal person, that legal person should be considered to be jointly owned and controlled by the individuals, and therefore also deemed sanctioned. Making funds or economic assets available to the legal person would constitute dealing with the sanctioned individuals.

US Sanctions Obligations

- Compliance professionals in firms subject to the US sanctions regime should assess whether a sanctioned individual or entity directly or indirectly owns an aggregate of 50% or more of a legal person. Where a legal person is owned by a sanctioned individual or entity, that legal person would also be deemed to be a sanctioned entity.
- When considering the control element of a legal entity under the US sanctions regime, compliance professionals should note where a legal entity is controlled by one or more sanctioned individuals or entities, then that legal person in not automatically sanctioned under the 50% rule.

UK Sanctions Obligations

- Compliance professionals in firms subject to the UK sanctions regime should look at ownership and control, however unlike the EU regime, compliance professionals would not simply aggregate the different holdings of multiple designated individuals in a legal person. Unless, for example, the shares or rights are subject to a joint arrangement between the sanctioned parties, or one party controls the rights of another, the holdings of multiple individuals should be treated as separate.
- Compliance professionals should also be aware that ownership and control also relates to holding more than 50% of the voting rights in a legal person.

Funding accounts held in sanctioned financial institutions

The obligation to screen beneficiary information in transactions has long been embedded in legislation and is well known by firms and compliance processionals alike. However, since the Russian invasion of Ukraine in February 2020, the UK Office of Financial Sanctions Implementation (OFSI) has issued five enforcement actions against firms in various industries as a result of said firms making funds available to designated persons without a licence.

In two such instances related to FinTech firms; enforcement actions were issued as a result of the firms in question sending funds to accounts held by their customers in a sanctioned bank. The customers were not designated individuals or entities, but transaction screening also applies to the beneficiary bank, not just the ultimate beneficiary of the transaction.

In the public notice related to one of the cases, the OFSI stated "OFSI considers that transferring funds to accounts held by non-designated persons with designated banks is a breach of the prohibition on making funds available to a designated person in the UK Regulations if the person knew, or had reasonable cause to suspect, it was doing so. Companies and individuals must therefore ensure they carry out due diligence on the banks and financial institutions involved in transactions, as well as all other parties in the transaction, to ensure they do not breach financial sanctions[1]".

Timing of Sanctions Reviews

In a separate enforcement action in August 2023, the OFSI used its new Disclosure enforcement power for the first time. In this case, a FinTech firm permitted a cash withdrawal from a business account owned or controlled by a designated person.

The firm's policy at the time of the breach was to put a block on the customers' accounts to stop credits and debits from being processed on the account. However, the policy allowed cardholders associated with the account to access funds from that account. It took the firm several days to work the alert and determine that the alert was a true hit.

In the associated public notice the OFSI stated that *"Companies and individuals must ensure they do not make funds available to designated persons or entities owned or controlled by designated persons."*

The firm's "policy at the time of the breach (of not restricting debit cards where a possible name match to a designated person was identified) was inappropriate in managing sanctions risks. A lack of staff availability to review sanctions alerts at weekends also led to a material delay in the proper restrictions being placed on the Designated Person's account and debit card[2]".

The OFSI notice further states:
"This case demonstrates that firms should carefully consider what steps are appropriate to manage their sanctions risk exposure. When a firm identifies a sanctions risk, it should take steps to fully address that risk by promptly restricting all forms of access to funds or economic resources. Firms should also maintain proportionate sanctions screening and alert review functions including, for example, at weekends where they conduct business at such times."

Geo location and IP address checks

Since the start of 2022, OFAC has published thirty enforcement actions, several of which have been as a result of insufficient controls related to Geo location and IP address checks.

In November 2023, OFAC published an enforcement notice relating to a US payments firm that provided digital or physical payment reward card programs for corporate, non-profit and government clients through an online platform.
These programs allow the payment firm's customers to issue payment cards to select recipients, typically as part of a loyalty, award, or promotional incentive for employees, customers, and other beneficiaries. Upon receiving a list of card recipients from a customer, including names and email addresses, the payment firm would send an email containing a token to each authorized user, inviting each user to redeem the token for a prepaid card.

To redeem the token, users would navigate to the payment firm's website and provide their names, addresses, and email addresses. In a potential attempt to evade detection, certain users did not enter an address in a sanctioned jurisdiction, resulting in false-negative screening processes.

Once screened and verified, funds were released by the issuing bank to the users' prepaid cards and the cards would be issued by the payment firm to the users. The cards could then be used with participating merchants.

During a compliance review and subsequent investigation, the payment firm discovered it had redeemed prepaid cards for users with Internet Protocol (IP) addresses located in Iran, Syria, Cuba, and Crimea. After a further review, the firm identified that it had redeemed prepaid cards for additional card recipients who, during the redemption process, had used email addresses with suffixes (sometimes called top-level domains) associated with sanctioned jurisdictions (e.g. Syria is .sy, Iran is .ir)

Once the reviews were concluded, the payment firm had processed 12,391 redemptions totalling $549,134.89 on behalf of cardholders located in, or potentially associated with, sanctioned jurisdictions.

In the associated public notice, OFAC stated *"This enforcement action underscores the importance of obtaining and using all available information to verify a customer's identity or residency, including by using location-related data, such as IP address and top-level domains, for sanctions compliance purposes. As appropriate, firms providing services through online platforms should integrate such information into a risk-based sanctions compliance program to prevent the provision of services to persons in sanctioned jurisdictions. This case further demonstrates the potential shortcomings of controls that rely on customer-provided information, rather than a holistic information-gathering system that can mitigate evasion or misrepresentation. The action further highlights the value of conducting proactive, self-initiated reviews to identify compliance gaps, disclose any potential violations to OFAC, and taking steps to remediate deficiencies, including by instituting periodic independent testing to ensure adequate controls[3]".*

In a separate case in September 2022, OFAC published an enforcement notice relating to a US payments firm. The firm in question supplies and distributes rewards, often in the form of stored value cards, to support its clients' employee and customer incentive programs. The firm serves two primary roles in the rewards life cycle; initially during the issuance process the firm provides awards to recipients via email; and, the firm facilitates the redemption process, enabling recipients to click on a reward link and use the rewards to make a purchase.

A review conducted by the firm identified that several reward recipients' email addresses had top line domains associated with sanctioned jurisdictions. Between 2016 and 2021 the firm transmitted 27,720 merchant gift cards and promotional debit cards totalling $386,828 to individuals with email or IP addresses associated with Cuba, Iran, Syria, North Korea or Crimea.

While the firm used geolocation tools to identify transactions involving countries at high risk for fraud, and had OFAC screening and KYB mechanisms in place, it did not use these controls to identify whether recipients of rewards, as opposed to senders of rewards, might involve sanctioned jurisdictions.

In the associated public notice, OFAC stated *"This case demonstrates the importance of using relevant geographic information as part of an effective, risk-based sanctions compliance program, including the use of appropriate geolocation tools to identify transactions potentially involving sanctioned jurisdictions. In addition, while contractually obligating customers to comply with sanctions regulations can help mitigate risk, it does not obviate the need to impose other sanctions compliance controls when appropriate on a risk basis[4]".*

Employee Training

In July 2022, OFAC published an enforcement notice relating to a banking institution that issues credit and debit cards to individuals and business.

In 2012, an individual applied for and obtained a supplemental credit card on an account maintained by a U.S. person. In May 2018, OFAC designated this individual as a sanctioned person and added them to OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List).

A few days after OFAC designated the individual, the bank's internal sanctions list screening system generated a "high confidence" alert, which was erroneously closed by an operations analyst responsible for conducting the initial review of the alert, despite a match against multiple data elements (name, date of birth, and National ID number). The bank also failed to complete an internal procedural requirement for a second-level review for all high-confidence alerts.

In June 2018, a bank employee investigating an anti-money laundering media alert identified and escalated the individual's connection to the account. The next day, instructions were given to immediately suspend charge privileges on all cards linked to the U.S. person's account, including the individual's supplemental card. However, the employee who entered the suspension code into the system did not include comments indicating that the restriction was sanctions related. As a result, when the U.S. person accountholder called the following day to inquire about the account status, a customer care professional removed the suspension.

The bank's AML team caught the error the following day and directed the account to be re-suspended. However, the team that carried out this task mistakenly applied the incorrect suspension code, which allowed the account to conduct seven additional transactions after the suspension was lifted in June 2018 and before the account was closed in July 2018.

In sum, between approximately May 2018 and July 2018, the bank processed 214 transactions totalling $155,189.42 involving the account.

In the associated public notice OFAC stated *"This action highlights the importance of properly training*

employees on sanctions compliance procedures and ensuring that those procedures are followed appropriately, especially when high confidence alerts are generated. Also, consistent application of enterprise-wide compliance measures, including controls to prevent other departments or personnel from overriding a sanctions-related decision to suspend an account, can also help mitigate the risk of a sanction's violation[5]".

Wilful Blindless or Deliberate Failure?

In a recent case that continues to unfold, a virtual currency exchange based in the Cayman Islands reached a settlement to pay $968,618,825 to resolve potential civil liability relating to 1,667,153 apparent violations of multiple sanctions programs administered by OFAC.

The violations occurred between August 2017 and October 2022, involving virtual currency trades on its platform with users from sanctioned jurisdictions or blocked persons, despite projecting an image of compliance. The senior management knowingly permitted U.S. and sanctioned jurisdiction users on the platform, disregarding sanctions risks.

The settlement amount reflects OFAC's determination that the violations were not voluntarily disclosed, and the conduct was egregious. The company also reached separate settlements with the Department of Justice, FinCEN, and the Commodity Futures Trading Commission. The total settlements amount to over $4 billion, and the firm's CEO has also stepped down and pleaded guilty to money laundering.

In the associated public notice, OFAC states *"Compliance personnel must be empowered and receive the backing and authority necessary to effectively fulfil their function. A culture of compliance, where senior management is invested in and supports an organization's program and allows it to operate effectively and without undue interference, is essential to avoid committing violations of OFAC sanctions[6]".*

Conclusion

In conclusion, the complexity of sanctions compliance, magnified by geopolitical events, requires a proactive and adaptable approach from compliance professionals. It extends beyond mere screening processes and demands a comprehensive understanding of jurisdiction-specific nuances. Senior compliance professionals must champion a culture of compliance within their organizations, ensuring that policies, procedures, and controls effectively manage the sanctions risk associated with their business operations. The lessons learned from enforcement actions and evolving regulatory landscapes should serve as catalysts for continuous improvement in the field of sanctions compliance.

REFERENCES
1. OFSI Penalty Report
2. OFSI Disclosure
3. https://ofac.treasury.gov/media/932276/download?inline
4. https://ofac.treasury.gov/media/928326/download?inline
5. https://ofac.treasury.gov/media/924406/download?inline
6. https://ofac.treasury.gov/media/932351/download?inline