SANCTIONS MASTERCLASS SERIES
FOLLOW-UP BRIEFING PAPER

HOW TO NAVIGATE THE DIGITAL AND TECHNOLOGY LANDSCAPE

Background

In January, ACAMS hosted a Sanctions Masterclass on ‘How to Navigate the Digital and Technology Landscape’. The session formed part of the 2021 Masterclass series and was developed in conjunction with Melissa Duffy, Dechert LLP, and Sean Kane, PayPal. The Masterclass attracted more than 4,000 registrations and generated a large number of live questions.

Our purpose in producing this paper is to build upon the information provided in the Masterclass by outlining the challenges in sanctions compliance for the digital and technology sector and to identify key considerations to assist compliance individuals in effectively navigating this landscape as it evolves. The below should be read in conjunction with viewing the Masterclass and downloading the accompanying slides.

As a reminder the free on-demand version of the Masterclass is available here.

Masterclass Overview - Sanctions Requirements in the Digital and Technology Sector

The Masterclass was split up into three parts, the first of which was presented by Melissa Duffy and Sean Kane, and provided an overview of the sanctions and related export controls that are particularly important for the digital and technology sector. The second part focused on six short case studies, and provided a number of scenarios which demonstrated the applicability of the sanctions and export controls introduced in the first part. Polling questions were used to ascertain the audience knowledge and views of the sanctions risks that were presented in each case study. Once the polling had been completed, analysis of the sanctions risk in each scenario was provided. The final section was the presentation of four longer case studies that highlighted the complexity of complying with multiple sanctions and export controls requirements depending on the activity in
question. Shorter versions of the case studies in the Masterclass have been adapted for use in this paper.

It is important to keep in mind that sanctions compliance expectations in the digital and technology sector have continued to expand with different, and evolving, requirements creating a complex risk environment. By its very nature, the continual innovation and technological improvements of the sector present new and unprecedented compliance challenges, as well as new opportunities for managing risk. Within this paper, we set out the key risks and considerations for this sector, and examples will be provided of how they apply in practice. These were all discussed during the Masterclass.

For the purposes of this paper, the digital and technology sector is taken to include digital software, web-based platforms, cloud computing, applications, technology products, and associated services.

**Key Questions to Consider for Sanctions Compliance in the Digital and Technology Sector**

In terms of structure, this paper will follow similar themes to those covered within the Masterclass. These themes are centered around a number of key questions which need to be assessed in order to analyze sanctions risk exposure in the digital and technology space, including:

- Which sanctions regimes apply, based upon the origin of the products and services, the identities of the counterparties, and any other jurisdictional nexuses?
- Are any sanctioned parties or countries involved?

**Navigating the Sanctions Landscape for the Digital and Technology Sector**

**The Complex World of Sanctions and their Jurisdictional Scope**

Sanctions risks and compliance considerations can look different in different sectors. While there are common compliance themes across sectors, the issues for the digital and technology sector vary from those that apply to the regulated financial sector. Consequently, companies in the digital and technology sector need to understand the specific issues and compliance best practices that are unique to their operations. Key differences to be aware of include:

1. Sanctions are not just triggered by financial transactions but can come into play with the provision of services or the delivery of goods, even if no payments are involved (e.g. free software trials or returns and repairs on products).

2. Companies in the digital and technology sector have to contend with both sanctions and similar export control restrictions in the form of export bans on prohibited parties and embargoed countries. There are different triggering points for the application of sanctions (e.g. US person nexus) versus export controls (e.g. US origin goods, there is no need for US persons to be involved).
3. Transactions in the digital and technology sector can be very complex, for example, with multiple parties involved in a distribution channel. This creates unique challenges for customer due diligence and screening, which require compliance measures that match the business model.

A theme that is common across sectors is the fact that different jurisdictions have different approaches to sanctions (and export controls), and this can create conflicts of law.

This is particularly true of the digital and technology sector, as it is common for research and development, sales of technology products, and access to web-based services and applications to be provided on an international basis. While there often are multilateral efforts to coordinate, there often can be variations in how sanctions are implemented among the United Nations (UN)/European Union (EU) and their member states, the United States (US), the United Kingdom (UK), and other jurisdictions. Notably, the country that goes the furthest in its use of sanctions, embargoes and export bans on prohibited parties is the US. Because of the US’ far-reaching approach to sanctions and export control jurisdiction over US persons and products located abroad, multinational companies in the digital and technology sector often find they have to contend with US trade controls as a baseline, in addition to the local jurisdictions where they are operating.

Some jurisdictions have blocking regulations in place which prohibit complying with certain sanctions whilst in the local country or jurisdiction. These are put in place to stop the extra-territoriality of specific sanctions and to protect local business interests. For example, both the EU and UK prohibit persons and entities from taking certain actions to comply with US sanctions on Iran and Cuba. Also, recently, the Chinese government issued a blocking rule that provides the framework for companies in China to refuse to comply with extraterritorial US trade restrictions. Moreover, some jurisdictions have taken retaliatory action against jurisdictions that impose sanctions against them. For example, China has recently imposed sanctions against individuals and entities from the US, UK, EU and Canada. In addition, China implements import controls applicable to the digital and technology goods sector (e.g. restrictions on the importation or use of foreign encryption), which can make access to the local market challenging for US and multinational companies. Companies operating in such jurisdictions where there is blocking legislation often find themselves in the difficult scenario of having to navigate conflicts of law and arriving at creating commercial solutions to remain in compliance with applicable requirements.

**Expansive Scope of US Jurisdiction**

US sanctions are far-reaching and have broad scope of applicability, and this is no less the case with regard to export controls. Understanding what triggers US jurisdiction, and how it impacts digital and technology goods and services, is key to ensuring robust sanctions compliance.

---

1 Including entities incorporated outside the United States but owned or controlled by US persons, as well as certain foreign-made items incorporating US content or based on US technology/software.
US sanctions jurisdiction applies to all US persons\(^2\), wherever they are located. In addition, US sanctions jurisdiction can extend to non-US persons where they involve US persons in a transaction. This is often referred to as a US nexus and can be triggered where a non-US company involves US banks or US technology providers in facilitating transactions. In terms of the digital and technology sector, non-US companies need to be alert to a US nexus in their business.\(^3\) From the export control perspective, if any goods, software or technology are considered a US-origin item, then they will be subject to US export regulation, even if located abroad and possessed by foreign persons.\(^4\) If there is any US element to the business being undertaken, then compliance with applicable US sanctions and/or export controls will be required.

### Case Study: US Goods Produced in China

Goods that are sold by US companies but produced locally in China may still be subject to US jurisdiction. For example, high performance semiconductors based on US sensitive controlled technology will still be subject to US jurisdiction and considered a US good, even if they are made in China. Equally, they will also be considered a US good if they have a level of US origin-controlled content.

US sanctions are principally administered and enforced by the Office of Foreign Assets Control (OFAC) at the US Department of Treasury. The specific prohibitions that might apply to any transaction over which OFAC has jurisdiction will depend on the sanctions program implicated – for instance, certain transactions involving Iran might be treated differently to those involving Cuba. Given the complexity of US sanctions and OFAC’s expansive jurisdiction, any company operating in the digital and technology sector should identify any US nexus to their business and, as appropriate, implement appropriate controls.

For example, if a Software-as-a-Service tool is used by an entity outside of the US but is hosted on servers maintained by an entity within the US, then this will require compliance with US sanctions. Organizations must ensure servers located in the US are not engaging with US sanctioned parties or countries. A recent example of this is the case of Société Internationale de Télécommunications Aéronautiques SCRL (SITA).

---

\(^2\) This definition includes US nationals, foreign nationals located in the US, companies organized under US law and their overseas branches (or in the case of Cuba and Iran sanctions, a foreign owned or controlled subsidiary of a US company), or foreign businesses operating in the US.

\(^3\) For example; US citizen or Green card employees, USD payments that will clear the US financial system, US-based IT networks, server and systems, cross-border research and development, US technology support services, and US origin components in the supply chain.

\(^4\) (i) US origin, (ii) located in US (e.g. foreign origin software/data stored on a US server), (iii) foreign-made with certain levels of US content, and (iv) certain foreign-made items based on controlled US technology or software.
Compliance with Export Controls

Companies in the digital and technology sector must also ensure that they are in compliance with applicable export controls. Goods related to the digital and technology sector are often subject to export controls due to their nature. Export controls are government restrictions on the transfer of goods, software and technology for reasons relating to national security and foreign policy. Government export authorization may be required for an item depending on the control classification of the item (i.e. the type of control that applies), the destination, the end use, and the end user.

Case Study: Société Internationale de Télécommunications Aéronautiques SCRL (SITA)

In February 2020 SITA were subject to an Office of Foreign Assets Control (OFAC) Enforcement Action. The company in question, SITA, is a service provider to the civil aviation industry. In this case, OFAC determined that SITA had provided a variety of services to OFAC designated airlines using services and software that was subject to US jurisdiction. Specifically, the messaging services went through the US, some systems were hosted in the US, and some of the software was of US origin. Accordingly, even though SITA itself is not based in the US or deemed a US person, they were subject to US restrictions and agreed to pay a fine.

Case Study: US De Minimis Content

A technology company based in the UK has a UAE subsidiary that has been re-exporting test measurement equipment to Iran. Upon further inquiry, the company confirms that the equipment contains US origin semiconductors subject to export controls, amounting to 20% of the value. As an embargoed destination, the ‘de minimis’ US content threshold for Iran is 10% - therefore if any foreign-made good has over 10% US controlled content then it will be prohibited for Iran.

Many countries have export control requirements, and while there is international coordination, they do vary among jurisdictions. Thus, you should be aware of which goods are subject to what types of export controls in any country in which your company operates. For example, many jurisdictions (the US, EU, UK and many others) maintain coordinated military and dual-use list-based export controls. However, the US goes further with a range of unilateral controls on various items, use of regional embargoes, military end-use restrictions in certain countries with respect to commercial items, and list-based export bans against specific individuals and entities.
Export controls in the US are managed by the Bureau of Industry and Security (BIS), a part of the US Commerce Department. BIS implements the Export Administration Regulations (EAR), the legal framework which determines whether a person may export something from the US, whether it can be re-exported from a third country or whether it can be transferred. The EAR applies to goods/commodities, software and technology. US export jurisdiction is far-reaching, and most companies operating in the global technology sector deal in at least some items (in their production equipment, supply chain, software components, etc.) that are subject to US export jurisdiction.

**Key Sanctions Compliance Considerations Covered in the Masterclass**

Firstly, it is important to make sure that you know who you are doing business with. It is key to undertake due diligence into who and where the end-user of a good or service is going to be, and what it will be used for. It may be good practice to build into your contracts representations and warranties, where applicable, that state that goods cannot be provided to any sanctioned parties or in any sanctioned jurisdiction.

Obtaining thorough information about a transaction will enable a full review to be undertaken to understand the sanctions and export control implications. All parties involved can also be screened to determine whether there are any links to sanctioned parties.

**Case Study: Software as a Cloud-Hosted Service (SaaS)**

A US-based company with global operations provides web-based communications services for a monthly subscription fee. The software uses strong encryption that is highly export controlled. Customers may create an account, log-in, and access your software as a cloud-hosted service (SaaS). Customers cannot download, install, or access source code.

It is discovered that its Russian subsidiary has been licensing user rights to customers in Crimea, and to parties in Russia on the OFAC SDN and Sectoral Sanctions lists, as well as the BIS Entity List.

As customers in Crimea and on the OFAC SDN List are accessing the US-based platform, this would be the provision of a service to sanctioned parties. Therefore, US sanctions apply.
Secondly, it is also key to establish where all parties are based and where they are going to be accessing any systems, servers, or goods from. If there is any connection to a sanctioned jurisdiction this will need to be reviewed. The use of Internet Protocol (IP) tracking may also assist in establishing where digital products and services are being accessed from. Some companies may decide to block certain IP addresses in order to remove access to their products and services from specific jurisdictions that are subject to sanctions. A recent example of this is the case of BitGo, Inc.

Thirdly, as has already been covered in this paper (but needs to be emphasized again), ensure you take into account the continued applicability of US jurisdiction and therefore US sanctions and export controls.

Fourthly, periodic rescreening of customers that receive ongoing support and services, and tracking what they are receiving, is important, as a customer’s sanctions status could change overnight.

Case Study: Ongoing Support/Warranties

A US based company realizes it has been shipping satellite equipment to Syria indirectly through an intermediate customer. The US based company has continued offering support and training, as part of the business relationship. Therefore, not only has there been a breach of OFAC sanctions in relation to Syria by shipping the equipment, there have been continuous breaches by providing ongoing support to parties in Syria.

Case Study: BitGo, Inc

In December 2020, BitGo Inc was subject to an OFAC Enforcement Action for failing to prevent individuals from using their digital wallets whilst based in OFAC comprehensively sanctioned jurisdictions. OFAC deemed that BitGo had reason to know that their users were located in the OFAC comprehensively sanctioned jurisdictions through IP address data on the devices used to log in to the BitGo platform. However, at the time BitGo didn’t have any controls in place to prevent access by these users in those jurisdictions and therefore were found to have breached OFAC sanctions. As a result of the enforcement BitGo committed to putting IP blocking (as well as specific email restrictions) in place for those jurisdictions.
Finally, it is important to have some form of a sanctions and export compliance program in place. In May 2019 OFAC published its guidelines⁵ on ‘what a good sanctions compliance program looks like,’ and BIS maintains similar guidance.⁶ This is a very useful tool to help shape a company’s compliance framework. This framework has also been cited in several enforcement actions by OFAC.

**Key Takeaways from the Masterclass**

In addressing the sanctions risk in the digital and technology sector the following themes stood out from the Masterclass:

1. Always know who you are doing business with and where they are based so that you are able to ascertain which sanctions apply and whether you are dealing with a sanctioned party

2. Identify the origin of any goods and services you are dealing with and where they are being shipped to for export control considerations and to establish whether there are any sanctioned jurisdictions involved

3. Always factor in the reach of US jurisdiction to establish whether any of the products, third party products or parties are subject to US jurisdiction

4. Establish where parties are going to be accessing any systems, servers, or goods from; if there is any connection to a sanctioned jurisdiction this will need to be reviewed

5. The complexity of the multiple sanctions programs that may apply to your business making it a challenge to comply with all relevant requirements

6. Constant reviews of all your customer relationships for sanctions implications, especially where there is the provision for ongoing support, service, and warranties

7. It is important to establish where your technology is actually located to evaluate sanctions and export control considerations

8. It is key to consider the use of blocking certain IP addresses in order to block access to certain products and services from OFAC comprehensively sanctioned jurisdictions

It is crucial to keep in mind all of these key points when undertaking business in the digital and technology sector to ensure you are complying with the ever growing and complex world of sanctions regulations and export controls.

---


About ACAMS

ACAMS is the largest global membership organization for Anti-Financial Crime professionals, with 82,000+ members in over 175 countries.

ACAMS offers two exclusive programs for sanctions professionals – the internationally recognized Certified Global Sanctions Specialist (CGSS) accreditation, and (brand-new in 2021), the Sanctions Compliance Foundations online certificate.

Also available to sanctions teams and professionals is the ACAMS Sanctions Space, led by Dr Justine Walker and our International Sanctions Compliance Task Force. The Sanctions Space is a comprehensive and dynamic resource center, encompassing Masterclasses, Global Monthly Update briefings, authoritative Whitepapers and a podcast series telling the stories behind the sanctions.

Learn more about Sanctions at ACAMS at acams.org/sanctions

Ashley Campbell, Global Sanctions Secondee

April 2021

Upcoming 2021 Masterclass Program

May 18, 9:00am EDT/2:00pm BST/3:00pm CEST: Investment and Securities - Understanding Scope and Exposure

Those operating in the investment and securities marketplace face specific and complex sanctions risks which need be taken into consideration to ensure robust compliance. With increasing numbers of sanctions measures impacting these assets across a number of sanctions regimes, it is more important than ever to understand both the scope of these measures and your exposure. Join our expert panel of financial sector and legal experts as they explore these matters in this in-depth masterclass, which will also feature a live Q&A.

June 22, 2021: Nexus of Cyber, Ransomware and Sanctions Compliance

July 20, 2021: Jurisdiction & Sanctions Regime - Rapid-Fire Update

August 17, 2021: Sanctions Screening Models and Key Validation techniques

September 21, 2021: Jurisdiction & Sanctions Regime - Rapid-Fire Update

October 19, 2021: Risk Managing Personal Remittances, Humanitarian Transactions and Permissible Payments into Highly Sanctioned Jurisdictions

November 16, 2021: Proliferation Financing and Strategic Trade Controls - Assessing and Managing Risk

December 14, 2021: Jurisdiction & Sanctions Regime - Rapid-Fire Update