NEW SANCTIONS REPORTING OBLIGATIONS ON CRYPTOASSET PROVIDERS

Sep 12, 2022

SUMMARY

On 30 August 2022, two new statutory instruments that amend existing sanctions legislation and target cryptoasset businesses came into force. The Regulations extend reporting obligations under the UK’s sanctions regime to cryptoasset businesses; bringing them expressly within the remit of the Office of Financial Sanctions Implementation (OFSI) for reporting purposes. Cryptoasset exchange providers and custodian wallet providers must act now to ensure compliance to avoid the risk of civil or criminal penalties. We consider the regulatory changes and practical steps that affected cryptoasset businesses can take to minimise risk and ensure compliance.

BRINGING CRYPTO-ASSET BUSINESSES INTO THE SANCTIONS REGULATORY FRAMEWORK

An unprecedented amount of sanctions legislation has been introduced by the Government (a) in response to Russia’s actions and (b) as part of concerted efforts to tackle illicit finance in the UK. As the regulatory framework develops, so too have the sophisticated attempts to circumvent it. A growing concern has been the use of cryptocurrencies as a means to evade sanctions. The introduction of the Sanctions (EU Exit) (Miscellaneous Amendments) Regulations 2022 and the Sanctions (EU Exit) (Miscellaneous Amendments) (No.2) Regulations 2022 (the “Regulations”) is a direct response to this.

EXISTING LEGISLATIVE PROVISIONS

Under the majority of the UK’s autonomous sanctions regimes made under s1 of the Sanctions and Anti-Money Laundering Act 2018, a “relevant firm” is under an obligation to notify OFSI as soon as reasonably practicable if, in the course of its business, it knows or reasonably suspects that:

- A person, whether natural or legal, is subject to UK financial sanctions (a “designated person”); or
A person, whether natural or legal, has committed a breach of the financial sanctions provisions (such as making funds or economic resources available to a designated person).

Where such a notification is made to OFSI, a relevant firm must include within the notification:

- The information or other matters on which the knowledge and suspicion is based;
- Any information it holds regarding the person by which the person can be identified and, where the designated person is also a customer, the nature and amount or quantity of any funds or economic resources (including cryptoassets) held.

**EXPANDED MEANING OF ‘RELEVANT FIRM’**

The Regulations expand the definition of relevant firm, such that, for the purposes of these notification provisions, they include cryptoasset exchange providers and custodian wallet providers (“crypto asset businesses”). For these purposes:

- a “cryptoasset exchange provider” is a firm or sole practitioner that exchanges, or arranges or makes arrangements to exchange cryptoassets for currency (fiat or digital) or which operates a machine automating the exchange process;
- a “custodian wallet provider” provides services which safeguard and/or administers cryptoassets or private cryptographic keys for customers to hold, store and transfer cryptoassets.

**TERRITORIAL EXTENT**

The territorial reach of each individual autonomous sanctions regime is set out in the statutory instrument giving rise to it; each of which refers to conduct taking place here or abroad on the part of a ‘United Kingdom person’. It encompasses UK nationals, or bodies incorporated or constituted under the law of any part of the UK but would appear to exclude cryptoasset businesses comprising non-UK nationals incorporated elsewhere.

For UK-based cryptoasset businesses, and UK nationals operating in businesses registered elsewhere, the expansion of this definition brings them into OFSI’s regulatory remit (many of them for the first time). This is significant from both a criminal and a civil perspective.

**BREACH OF THE REPORTING REQUIREMENTS**

Breach of the reporting requirement means that crypto asset businesses could be subject to enforcement actions provided for within the various regimes.

Persons that fail to comply with reporting obligations will commit an offence punishable on summary conviction by up to six months imprisonment and/or a fine. For body corporates, the
sentence will be an unlimited fine. Where a body corporate is prosecuted, a director, manager, secretary or other similar officer of the corporate can be held liable as an accessory on the basis of consent, connivance or neglect. Successful criminal prosecution relies on proof that a person had the requisite mens rea at the time of the act which forms the basis of the offence.

OFSI has the power to impose civil monetary penalties for failures to comply with obligations imposed under sanctions legislation, which include the reporting obligation. The monetary penalties can be significant. The enforcement of civil breaches of sanctions legislation is possible on a strict liability basis.\[2\]

**PRACTICAL STEPS**

It is important that affected cryptoasset businesses act now. Whilst they should not ignore low risk areas, the strongest focus should be on where the greatest risks are; for most, it will likely be during the customer onboarding, know-your-customer (“KYC”) process.

In preparing for these changes, cryptoasset businesses should ensure that:

- Robust and appropriate policies and procedures are in place to identify when notifications to OFSI should be made, as well as how to make such notifications;
- Written policies are available and circulated to front-line staff in an easy-to-read format – consider using diagrams and colour codes to highlight key risks;
- Training is regularly updated and available to front-line staff allowing them to evaluate risk on a case-by-case basis and continually assess the controls already in place;
- There is a clear process in place to deal with freezing assets and/or suspicious transactions, including how and when to communicate this to the customer;
- Detailed records of transactions, counterparties and correspondence are kept for audit purposes;
- Due to the fact that many customers of cryptoasset businesses will be onboarded remotely, consider enhanced due diligence processes to account for the lack of face-to-face checks, and accordingly have the necessary policies and controls in place;
- Exposure to financial sanctions within the KYC or due diligence process are assessed and appropriate steps taken to mitigate the risks, taking special account of customers who are known politically exposed persons; and
- Appropriate procedures are in place for staying up-to-date with the financial sanctions regimes and OFSI’s target lists and that staff are appropriately trained.
Legal advisors can assist in helping cryptoasset businesses to prepare. In addition to the new reporting and notification obligations to OFSI, where firms are registered for money laundering purposes and are involved in transactions that give rise to concerns regarding sanctions evasion, firms should give due consideration to their obligations to make a report to the National Crime Agency and their regulator.

We express our thanks to Kwabena Boateng, Trainee, who assisted in the production of this article.

[1] The exceptions, as at the date of writing are, the UK sanctions relating to (1) Syria cultural property (the Syria (United Nations Sanctions) (Cultural Property) (EU Exit) Regulations 2020, SI 2020/1233), and (2) the Lebanese bombing in 2005 that killed former Prime Minister Rafiq Hariri and others (the Lebanon (Sanctions) (Assassination of Rafiq Hariri and others) (EU Exit) Regulations 2020, SI 2020/617)

[2] Policing and Crime Act 2017, s 146 (as amended)

RELATED PRACTICE AREAS

- Anti-Money Laundering Compliance
- Financial Regulation Compliance & Investigations
- Financial Services Corporate & Regulatory Team
- Fintech
- White Collar

MEET THE TEAM

Daniel Csefalvay
London
daniel.csefalvay@bclplaw.com
+44 (0) 20 3400 4570