HERBERT SMITH FREEHILLS

Corporate Crime Briefing

Tackling economic crime in the UK: The Economic Crime and Corporate Transparency Bill

8 DECEMBER 2022
London

A new bill to tackle economic crime is currently progressing through the legislative process. The Economic Crime and Corporate Transparency bill (the **Bill**) was first laid on 22 September 2022 and is expected to receive royal assent in the coming weeks. Whilst the Bill remains subject to change as it continues to pass through Parliament, its key provisions are likely to remain relatively similar to those described below.

In this briefing we look at the Bill's proposed amendments to the Proceeds of Crime Act 2002 (**POCA**), including in relation to regulated sector reporting and information sharing, and cryptoasset confiscation and recovery, in addition to the Bill's proposed enhancements to the regulatory and investigatory powers of the Serious Fraud Office (**SFO**) and Solicitors Regulation Authority (**SRA**). We consider the practical implications of those proposals and the broader context of economic crime reform in the UK. The Bill also proposes very significant reforms to the role of Companies House, which are summarised in a separate briefing (available here).

We recently presented a webinar on all aspects of the Bill; any clients who missed the webinar and would like to listen to a recording can reach out to any of the contacts on this briefing or your usual HSF contact.

Table of contents

Related links

Herbert Smith Freehills

FSR and Corporate Crime Notes

Corporate Notes

1. Background to the Bill

The Bill follows hot on the heels of the Economic Crime (Transparency and Enforcement) Act 2022 (the **Economic Crime Act**), which was rushed through Parliament in March 2022 following Russia's invasion of Ukraine. The Economic Crime Act made various amendments to UK sanctions designation and enforcement, as well as the Unexplained Wealth Order regime (see our earlier briefing on those changes here). It also created a new Register of Overseas Entities holding UK property (the **ROE**), which is operated by Companies House (see our earlier briefing on the ROE here).

Rather like the Economic Crime Act, the current Bill contains a disparate selection of reforms to improve the UK's anti-financial crime framework.

2. Amendments to POCA: regulated sector reporting and information sharing; cryptoasset confiscation and recovery

Regulated sector reporting

If someone suspects that actions they intend to take may place them at risk of committing a money laundering (**ML**) offence, they can seek a 'defence against ML' (more properly, "appropriate consent") by making a report to the National Crime Agency (**NCA**) in relation to a proposed course of conduct (a **DAML request**). The NCA receives a significant volume of DAML requests every year. The Bill includes two exemptions to the requirement to make a DAML request – with a view to making the DAML system more efficient – both of which will be available to some or all[1] reporters within the ML-regulated sector (**regulated persons**).

- Firstly, under the 'exiting and paying away exemptions', a DAML request will not be required where a regulated person repays a customer up to £1,000 (or transfers property up to this value at a customer's direction) when terminating their relationship with that customer, provided certain conditions are met. One of those conditions is that the regulated person has complied with its customer due diligence obligations under Reg. 28 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the **MLRs**).

  Regulated persons will need to ensure they are comfortable they have complied with their obligations under the MLRs before relying on this exemption from the requirement to file a DAML request. It will remain necessary for regulated persons to file a suspicious activity report in relation to the suspected ML (under sections 330 and 331 POCA).

- Secondly, a DAML request will not be required in certain situations where suspected criminal property is mixed with other (non-suspicious) property. The Bill's explanatory note provides the example of a bank account containing a total of £5,000. Of this, £2,000 has been received legitimately from the accountholder's employer and £3,000 is believed by the bank to have been obtained through a fraudulent loan application. Under the new exemption, the bank will be permitted to allow the customer access to up to £2,000 of their funds without needing to make a DAML request. In other words, the account can continue to be operated, provided the account balance does not dip below £3,000. At present, views vary as to whether the entire account must be frozen in this situation, or whether a 'ring-fencing' approach is permissible – a subject which was canvassed in the Law Commission's SARs Regime Consultation in 2018.

  The fact that HM Government (**HMG**) is attempting to address the long-standing issue of fungibility/mixed funds is welcome. There may however be some practical challenges involved in seeking to rely on this exemption. In particular, these include: (i) that the identification of suspected criminal property may be less clear-cut than the example included in the Bill's explanatory note, particularly where there are several examples of potentially suspicious activity in an account over a period of time; and (ii) there may be operational challenges in ensuring that property held in a customer's account does not drop below the value of the suspected criminal property.

Regulated sector information sharing

The Bill includes new voluntary information sharing provisions between certain members of the regulated sector, which are intended to help prevent rogue customers from moving between different firms. The Bill

[1] Some parts of the regulated sector may be excluded from the scope of the exceptions by statutory instrument.

affords protection from a breach of confidentiality obligations or civil liability[2] to a customer where information is shared:

- Directly by one regulated person (**RP1**) with another regulated person (**RP2**), where, either: (i) RP2 requests the information, having reason to believe that RP1 holds information that will assist RP2 in carrying out certain financial crime compliance activities (**relevant activities**); or (ii) RP1 has decided to take a safeguarding action (i.e. terminating the relationship or refusing or restricting access to products or services) due to concerns about economic crime, provided that (in either case) RP1 believes that the information sharing will assist RP2 in its relevant activities; or
- Indirectly between RP1 and RP2 via a third party intermediary (**TPI**), e.g. a database/platform, perhaps similar to CIFAS, the fraud-information sharing service.

Notably, the Bill (as currently drafted) specifies that it does not afford any protection from liability arising for any breach of data protection legislation. This may result in a practical impediment to regulated persons' reliance on these provisions, for example if they do not consider there is sufficient clarity that there is a lawful information gateway under data protection legislation.

Cryptoasset confiscation and recovery

To address the increasing use of cryptoassets to move and launder the proceeds of crime, the Bill includes various amendments which are intended to enable law enforcement authorities (**LEAs**) to recover cryptoassets in broadly the same way as tangible assets.

Criminal investigatory and confiscation-related powers

- The Bill removes the requirement for an arrest to have been made before search and seizure powers can be used. This amendment will affect all property types but HMG have said this will be particularly useful in relation to cryptoassets.
- The Bill extends the various investigatory and enforcement powers under POCA to cover cryptoassets and "cryptoasset-related items" (i.e. items which are, or contain or give access to information that is, likely to assist in the seizure of any cryptoasset) explicitly.
- It will be possible (with a magistrate's court order) to require UK-connected cryptoasset service providers to realise cryptoassets that are subject to a confiscation order and to pay the proceeds to LEAs. **UK-connected cryptoasset service providers** are cryptoasset exchange providers or custodian wallet providers which: (i) are acting in the course of business carried on in the UK; (ii) have terms and conditions with customers which provide for legal disputes to be dealt with in the UK; (iii) hold data relating to their customers in the UK; or (iv) have their registered or head office in the UK and the day to day management of their business is the responsibility of that office or another establishment maintained by it in the UK.
- Cryptoassets which are subject to a confiscation order may be destroyed (rather than realised or released) if: (i) there are reasonable grounds to believe that the realisation of those assets would be contrary to the public interest (e.g. because they would likely facilitate future criminal conduct); or (ii) it's not reasonably practicable to realise them. This can be done where a magistrate's court order has been obtained. Third parties who have, or may have, an interest in the property will have the ability to make representations before such an order is made.

Civil investigatory and forfeiture-related powers

- The Bill introduces a new type of freezing order which can be sought where there are reasonable grounds to suspect that cryptoassets held in a wallet administered by a UK-connected cryptoasset service provider are recoverable or are intended for use in unlawful conduct. If imposed, the freezing order will prohibit any withdrawals or payments from the crypto wallet or any other use of the wallet for up to three years. This type of freezing order can be made without notice. There may be exclusions to permit the person by or for whom the crypto wallet is administered to meet their reasonable living expenses or to carry on any trade, business, profession or occupation.
- Secondly, reflecting the significant volatility affecting cryptoasset value, LEAs or the person from whom assets were seized can apply for a court order to convert assets into cash while civil recovery proceedings

[2] The Bill as introduced provided exemptions only for protection for breach of confidentiality, but this has been amended to introduce a broader protection during the Committee stage.

remain ongoing. This can be obtained where there are concerns that the assets may suffer a significant loss of value in the period before they are released or forfeited.

- In addition, similar to the criminal regime, forfeited cryptoassets may be destroyed where this is in the public interest or it is not reasonably practicable to realise them.

3. Amended regulatory and investigatory powers for the SFO and SRA

Amended SFO powers

The Bill extends some of the information gathering powers which can be used by the SFO. The stated aim is to enable the SFO to carry out the early stage of an investigation more promptly, to determine whether a crime has taken place or whether a case should be discontinued.

At present, the SFO is able to use its powers under section 2 Criminal Justice Act 1987 (**CJA**) (**section 2 powers**) to compel persons to answer questions and provide documents, and to apply for a warrant to search premises during investigations and, in respect of international bribery and corruption only, prior to opening an investigation. In international bribery and corruption cases, the powers can be used under s.2A CJA to determine whether to open an investigation. In respect of other types of crime, they can only be used after an investigation has been opened under section 1. The Bill amends section 2A CJA so that it can be used in respect of any type of crime, giving the SFO greater flexibility at the pre-investigation stage.

Amended SRA powers

The Bill proposes an amendment to the regulatory objectives of the SRA to include the promotion of the prevention and detection of economic crime. A further proposed amendment is intended to enhance the SRA's power to impose financial penalties in relation to economic crime by removing the current statutory cap of £25,000.

The proposed amendments follow on from the 2020 National Risk Assessment, which 'assessed' the legal services sector as presenting a 'high risk' in relation to potential ML abuse, fraud and breaches of sanctions legislation.

4. Commentary

The Bill builds upon the reforms introduced earlier this year by the Economic Crime Act. Its proposed amendments (as currently drafted) should enhance the regulatory and investigatory powers which can be used by LEAs in relation to economic crime. The Companies House reforms, not discussed in this briefing, are also significant and from a financial crime perspective are in many respects welcome.

There are however several matters which are not currently addressed by the Bill, which have prompted questions from some commentators as to whether it goes far enough.

Firstly and most importantly, all the powers in the world are of limited utility if LEAs do not have the resources to use them, and the criminal justice system more broadly is not adequately resourced. The House of Commons Treasury Committee and House of Lords Fraud Act 2006 and Digital Fraud Committee have both recently identified resourcing issues as a significant weakness in the effectiveness of the prevention and detection of economic crime. It will be interesting to see how next year's second Economic Crime Plan addresses the various challenges that the public and private sectors face in relation to economic crime, and how the UK will seek to address these.

Secondly, the Bill has received some criticism for not including reforms to corporate criminal liability (see our earlier briefing on this here). This is another area highlighted by the Treasury Committee and the House of Lords Committee – with the latter calling for the introduction of a new corporate offence of "failure to prevent fraud" which appears to be envisaged to be even broader than the reform 'options' that were proposed by the Law Commission earlier this year. On this issue, we disagree with the critics: it seems likely that reforms to corporate criminal liability will be forthcoming, but this is too important and complex an issue for an offence to simply be included in the Bill. Instead, further consideration of the Law Commission's proposals, and further consultation on the selected reform option(s), is needed. Those already watching the Bill's progression closely will know that Dame Margaret Hodge MP proposed the addition of a new corporate criminal offence of "failure to prevent economic crime" after the Bill was first introduced, but that amendment has since been removed. It

therefore appears unlikely that this issue will resurface in the Bill – but readers should continue to 'watch this space' more broadly.

5. Contacts

Susannah Cogman, Partner
+44 20 7466 2580
Susannah.Cogman@hsf.com

Dan Hudson, Partner
+44 20 7466 2470
Daniel.Hudson@hsf.com

Brian Spiro, Partner
+44 20 7466 2381
Brian.Spiro@hsf.com

Kate Meakin, Partner
+44 20 7466 2169
Kate.Meakin@hsf.com

Robert Hunt, Partner
+44 20 7466 3423
Robert.Hunt@hsf.com

Elizabeth Head, Of Counsel
+44 20 7466 6443
Elizabeth.Head@hsf.com

Ali Grodzki, Associate
+44 20 7466 6329
Ali.Grodzki@hsf.com

Eamon McCarthy-Keen, Associate
+44 20 7466 3776
Eamon.McCarthy-Keen@hsf.com

If you would like to receive more copies of this briefing, or would like to receive Herbert Smith Freehills briefings from other practice areas, or would like to be taken off the distribution lists for such briefings, please email subscribe@hsf.com.