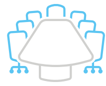
EVERSHEDS SUTHERLAND

Speed brief:

Keeping an eye on the economy

New provisions under the Economic Crime and Corporate Transparency Bill modifying POCA

*As part of its crackdown on serious financial crime, the UK government published the second Economic Crime and Corporate Transparency Bill (the **Bill**) on 22 September 2022. Of particular interest are the proposed changes to the Proceeds of Crime Act 2002 (**POCA**). We take an in-depth look at these changes, consider what the operational challenges might be and review the wider implications and potential risks for regulated firms.*



Introduction

The **first** Economic Crime (Transparency and Enforcement) Act (the **Act**) became law in March 2022. The Act was introduced to allow the government to move faster when imposing sanctions and created a register of overseas entities owning land within the UK to target foreign criminals using UK property to launder money, as well as reforming the UK's unexplained wealth order regime.

The Bill is the **second** part of the economic crime legislative package introduced by the Government. It delivers an additional range of reforms designed to tackle economic crime and improve transparency over corporate entities (you can read our summary of the reforms here). This briefing focuses on the proposed amendments to POCA, which appear to have largely gone under the radar but represent a positive step forward in tackling challenges caused by the current regime.

The Bill sets out two exemptions from the principal money laundering offences under POCA for regulated firms. It proposes to:

- increase the threshold amount for a defence against money laundering (**DAML**) from £250 to £1,000
- allow firms to pay away money or other property from a customer's account where they know or suspect that part of the funds or property is criminal property, if the amount in the account equals or exceeds the amount to which the knowledge or suspicions are held (i.e. ringfencing)

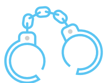
The Bill also sets out a new provision to address the shortcomings of the Criminal Finances Act 2017 which will allow firms to share information in the form of a direct disclosure regarding an existing or former customer for the purposes of preventing, detecting and investigating economic crime. We consider these amendments in more detail below.

The Bill is currently only in the Committee stage in the House of Commons. The Committee is scheduled to report back to the House by 29 November 2022.

What is POCA?

POCA creates three principal money laundering offences applicable to everyone in the UK (ss.327-329). Any person (natural or legal) may commit a money laundering offence if they deal with criminal property wherever they have developed knowledge or suspicion that it represents the proceeds of crime.

'Criminal property' is defined as all property, wherever situated, which constitutes or represents a person's benefit from criminal conduct and the alleged money launderer knows or suspects it is such a benefit. 'Criminal conduct' is conduct which constitutes an offence in any part of the UK, or which would constitute an offence in the UK.



What are the relevant offences under POCA?

POCA imposes additional obligations for the regulated sector. It creates 'regulated offences' for failing to disclose knowledge or suspicion of money laundering where the suspicion arises in the course of doing regulated business.

Employees must raise their suspicions internally to the Firm's nominated officer (often called the MLRO), who in turn is required to consider those suspicions and make a Suspicious Activity Report (SAR) to the National Crime Agency (NCA) as soon as practicable where there is knowledge, suspicious or reasonable grounds for suspicion of money laundering and terrorist financing. Firms should also freeze the accounts in question.

There is a separate offence of 'tipping off' (s.333A) which is committed if a person alerts an individual discloses to another person that a SAR has been filed and the disclosure is likely to prejudice any investigation that might be in progress or pending. Both the 'failure to disclose' offence and tipping off carry a possible sentence of unlimited fine and/or imprisonment for up to five years.

The threshold for reporting for the purposes of these offences is low. Suspicion has been defined as thinking *'that there is a possibility, which is more than fanciful, that the relevant facts exist'*. A *'vague feeling of unease'* is insufficient to trigger the requirement to disclose and the suspicion should be of a 'settled nature'.

Defences and exceptions under the current regime

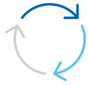
A firm may find itself in possession of, or need to handle or deal with, monies that it knows or suspects to be the proceeds of crime, whether directly or indirectly, in whole or in part.

In order to be able to deal with these funds, either to close the customer's account or to make payments requested by the customer, the firm should seek a DAML from the NCA to avoid committing an offence under POCA by paying away money or property. The NCA has an initial seven working days in which to refuse consent. If no refusal is received, the firm will be able to proceed with the activity it needs to undertake with a defence against committing a money laundering offence.

It's important to note that, currently, even where a relatively low value payment suspected to arise from criminal conduct is made into an account and co-mingled with other 'clean' funds in that account, all of the funds in the account must be considered tainted by the proceeds of crime and a DAML for the entire amount must be sought.

Under Section 339A of POCA, which applies only to deposit taking bodies (i.e. banks), a firm is permitted to process individual transactions or activity on an account where there is a suspicion of money laundering, so long as those transactions do not exceed £250, without the need to request a DAML. These 'threshold amount' transactions under £250 often fall into the category of 'lifestyle' payments such as regular household bills. Under section 339A(4) of POCA, the bank can apply to the NCA to increase the threshold amount on a case-by-case basis. However, this threshold is relatively low and does not often assist firms in closing accounts or making more substantial payments at the request of the customer. An explainer on the threshold amount more generally (and the ability to vary it) can be found here.

Under the current regime, despite the defences and exceptions above, regulated firms must comply with the POCA provisions summarised above. This can be particularly burdensome when trying to exit a customer or make payments from a customer's account which contains mixed clean funds and suspected criminal property. The proposed amendments are designed to both lighten the load on firms that often spend a significant amount of time and money trying to navigate the legislation, as well as reduce the burden on the NCA in dealing with a large number of DAML requests. During the period 2019/20, the NCA received 62,408 DAML requests, representing an increase of 81% on the previous year. The current figure is now likely to be even higher, given a huge corresponding rise in information SARs from 573,000 in 2020 to more than 900,000 in 2022.



Changes to the threshold amount

The Bill proposes to increase the threshold amount to £1,000. This means that a firm can pay away money up to this threshold without needing to seek a DAML as long as:

- the firm reports its suspicions of money laundering to the NCA in the usual way
- it complies with customer due diligence (**CDD**) duties before the act (i.e. the paying away of money) is done

The reference to CDD duties relates to the obligations on firms under the Money Laundering, Terrorist Financing and Transfer of Fund (Information on the Payer) Regulations 2017 (as amended) (**MLR**) to (i) identify the customer; (ii) verify the customer's identity; and (iii) assess and, where appropriate obtain appropriate information on the purpose and the intended nature of the business relationship or occasional transaction as well as a number of other obligations set out in Regulations 27 and 28 of the MLR. The provisions relating to the identification and verification of corporates and beneficial owners also apply in this context.

This requirement may prove difficult to satisfy in practice. In circumstances where a firm is in receipt of funds derived from criminal conduct, it is unlikely to be in possession of information regarding the purpose and intended nature of the transaction, or be able to obtain such information, as to be comfortable enough to pay out monies where it might risk committing an offence under POCA. It is also noted that many firms are currently undertaking significant remediation programmes to bring the level of CDD information presently held up to recent standards, particularly in view of a number of changes to CDD requirements over the last few years.

As such it is far from clear whether this amendment on its own will result in any meaningful change in the manner by which firms deal with suspicious activity. A request for a DAML may still be the most appropriate route in the circumstances given wider risks arising from first having to ensure full CDD information is held.

Changes to the ringfencing of funds

Separately, firms face significant challenges when they identify suspicious funds in an account that have been co-mingled with otherwise legitimate funds. In these circumstances, a firm must seek a DAML for the total amount within the account, rather than just the amount linked to the suspicious payments, preventing it from paying away any of the money in the meantime.

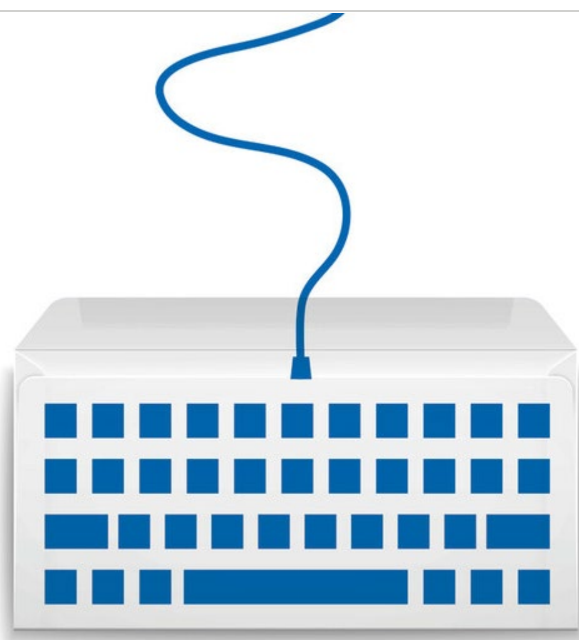
The Bill introduces an exemption to allow firms to pay away funds that the firm considers are legitimate even where these are co-mingled with dirty funds. This may include, for example, funds received by a customer through legitimate salary payments. This should enable regulated businesses to continue to allow customers to transact where money laundering is suspected, so long as the business *'keeps hold of property worth at least as much as the part of that property to which the knowledge or suspicion relates'* (noting that terrorist financing is excluded from these new provisions). In the event that the customer wishes to request an amount that exceeds the funds derived from legitimate sources, the firm is required to seek a DAML on the difference.

This marks a significant change to the current regime, and no doubt one that will be welcomed. A firm can often be stuck between the requirement not to commit an offence under POCA and the contractual requirement to make otherwise legitimate payments, such as salary payments. The failure to pay salary payments may create significant dispute between the firm and the irate customer who wants access to his money. These new arrangements will reduce the friction in such circumstances, albeit the changes may pose something of a challenge to implement in practice.

Interestingly, the explanatory note to the Bill includes a statement that the inability to ringfence up until this point has apparently resulted in *'disproportionate economic hardship to individuals unable to access their property, for example to pay rent or living expenses'* and should *'help reduce some of the disruption faced by customers'*. This feels, perhaps, an unlikely benefit for the government to emphasise to the advantage of the (potentially criminal) customer - after all, the reason the customer cannot access his money is because it is suspected of representing the proceeds of crime. More plausible is an eye on a reduction in DAMLs, the figures for which have never been higher.

In any event, these amendments, in conjunction with the changes to the threshold provision, are designed - in theory at least - make it easier for firms to allow the account to operate in a normal manner whilst also limiting the risk of tipping off. The practical effect of such reforms remains less certain. It is likely to be challenging to operationalise this approach - for example, how will a firm ensure that the portion of funds representing criminal property is not inadvertently paid away as a result of only partial blocks being applied to an account? The more risk-averse institutions may well decide that this approach brings new risks that are more simply dealt with by means of a complete DAML supported by a full block on the account.

Information sharing



At the moment, firms are limited in what can be shared with other firms about suspected economic crime in view of the duty of confidentiality owed to customers. This places real limits on the extent of any investigation into whether a transaction or activity more generally is suspicious, due to the inability to gather information from the counterpart to the transaction. It means that the firm can only see one side of a transaction which will typically mean it is not possible to have a complete picture on the wider activity. It also challenges a firm's ability to share broader information collected about customers that may go on to open accounts elsewhere. Existing information sharing provisions in the Criminal Finances Act 2017 have been ineffective to date.

The Bill will allow a firm to share information directly with another regulated counterpart where the information has been requested, or where a firm in possession of the relevant information has decided to take a safeguarding action, such as exiting a customer, as a result of concerns relating to economic crime. In these circumstances, a firm will not breach its duty of confidentiality to the customer where this information is shared in the specific circumstances set out below

Firms are only able to share information where the disclosure will assist the firm with a 'relevant action'. This is defined as:

- determining whether it is appropriate to apply CDD measures and the nature and extent of measure
- carrying out effective measures for identifying or verifying the identity of (or any other CDD measures) a customer or proposed customer

- determining whether it is appropriate to exit a customer of decline a product, service or transaction, or restrict the access of a customer

for the purposes of preventing, detecting or investigating economic crime.

These provisions will be voluntary and there is no positive requirement on firms to disclose information. Firms will need to be mindful to share data in a way that is compliant under data protection legislation, such as ensuring that a customer's data remains accurate and that it is used only for the purposes specified in the Bill. Firms must also disclose any suspicions to the NCA in the normal way.

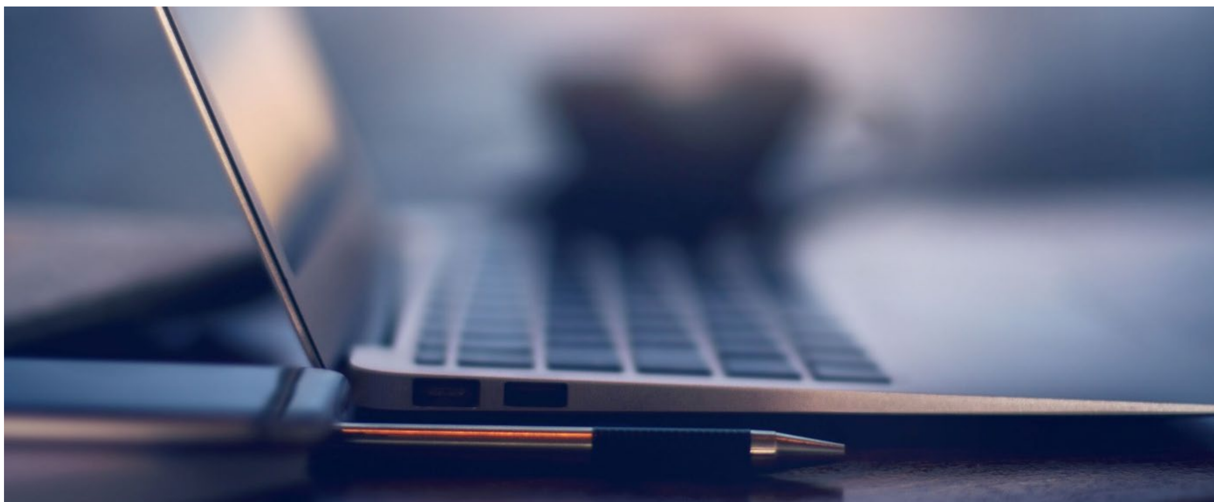
The Bill also proposes a method for the voluntary sharing of customer information between firms via a third-party intermediary. This is permitted where a firm has taken a safeguarding action and when the information may assist firms in carrying out 'relevant actions' in relation to the customer. The Impact Assessment that accompanies the Bill envisages the potential for a privately funded third party platform to facilitate the sharing of information, similar to National Fraud Database hosted by Cifas, where firms are able to share information where there is a suspicion of fraud.

Whilst the above provisions will better equip firms in investigating suspicions of criminal activity, they also create the risk of individuals becoming 'un-bankable', with firms refusing to onboard those exited from other firms for reasons relating to suspicions of financial crime. Indeed, many firms would consider it a challenge to explain to the regulator why risk appetite was set at such a level to allow it to take on such customers where it was aware of such apparent red flags.

Comment

The proposed changes take into account some of the challenges long faced by firms in dealing with suspicious activity. This collection of amendments is clearly targeted at improving on these well-known shortcomings in order to tackle financial crime without hindering other commercial activity. This ought to be a welcome development for firms. It nonetheless remains to be seen how the Bill will look after the Committee stage, and the proof will very much be in the pudding of the guidance (if indeed any is produced) to help firms understand how to operationalise these new rules.

In circumstances where the underlying regulatory AML regime is out of date, and SARs and DAMLs are higher than ever before, these amendments are unlikely to be the answer to any firm's prayers. Instead of tinkering, the government would do better to institute a long-overdue overhaul of the current regime to bring the UK's efforts to tackle money laundering up to date with today's financial services, products and systems.



Key contacts

Ruth Paley
Partner

T: +44 20 7919 0527
M: +44 734 270 8132
ruthpaley@
eversheds-sutherland.com

Steve Smith
Partner

T: +44 20 7919 0616
M: +44 758 461 5502
stevesmith@
eversheds-sutherland.com

Zia Ullah
Partner

T: +44 161 831 8454
M: +44 782 694 4979
ziaullah@
eversheds-sutherland.com

Anupreet Amole
Partner

T: +44 20 7919 4644
M: +44 757 250 3577
anupreetamole@
eversheds-sutherland.com

Jessica Hambly
Associate

T: +44 20 7919 0776
M: +44 788 103 7777
jesshambly@
eversheds-sutherland.com

eversheds-sutherland.com

© Eversheds Sutherland 2022. All rights reserved.
Eversheds Sutherland (International) LLP and Eversheds Sutherland (US) LLP are part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

cloud_uk\207949909\1