



connecting the future

**Economic Crime and Corporate Transparency Bill
HMT**

November 2022

Response from The Payments Association

Introduction

The Payments Association welcomes the opportunity to contribute to HMT “*Economic Crime and Corporate Transparency Bill*”.

The community’s response contained in this paper reflects views expressed by our members and industry experts recommended by them who have been interviewed and who are referenced below. As The Payment Association’s membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been drafted by Jane Jee, Lead of Project Financial Crime at The Payments Association. We would also like to express our thanks to HMT for their continuing openness in these discussions. We hope it advances our collective efforts to ensure that the UK’s payments industry continues to be progressive, world-leading and secure, and effective at serving the needs of everyone who pays and gets paid.

Please note that this is our final submission. It includes comments to the crypto section that were not included in the previous submission.

Tony Craddock
Director General
The Payments Association

Contents

BACKGROUND

The PA welcomes the Bill and is very pleased that some of the gaps and loopholes in current legislation are being addressed. The lack of proper corporate governance standards has enabled many millions to be laundered through the UK by corrupt states, criminal gangs and fraudsters. We agree that economic crime has reached a point where it is a threat to the UK's national security and negatively impacts the country's economy and opportunities for growth.

However, while the proposed new law is very welcome, as many experts have commented, without more resources for Companies House, the NCA, NECC and all involved enforcement agencies it will not succeed in its objectives and will not make a real difference to preventing financial crime. Implementation and enforcement are crucial as more information of itself will not lead to more a reduction in financial crime.

ABUSE OF CORPORATE STRUCTURES AND LLPs

The proposed reform of UK Companies House is particularly welcome. Companies and LLPs have been abused to move illicit finance for too long. LLPs need to be subject to the same requirements as corporates, as much as is practicable. The point was made in oral evidence that PSCs can be identified even in an LLP see also <https://www.transparency.org.uk/partners-in-crime-UK-LLP-Limited-Liability-Partnership-money-laundering-press-release>

Companies House will need to fundamentally alter its culture and mindset to become a proactive enforcement entity. As Chris Taggart said, this may be as just as important as their new powers. The current reality is that Companies house just forms legal entities (not necessarily businesses which contribute to the economy or are good for the country). Companies House now need to think digitally – for example there may be no downside to a Company being struck off if the criminals have already used the Company to fulfil their purpose. Companies House also need to recognise that shell companies can be a container for assets and may have no legitimate commercial or charitable purpose so that they only benefit criminals.

Companies House alignment with Anti-Money Laundering legislation and guidelines such as those of the JMLSG. It is important to ensure and strive for consistency and standardisation of data capture terminology across the industry within the UK, and other jurisdictions. For example, there is a need to align the definition and the record keeping of ultimate beneficial owners (UBOs) with Companies House Persons of Significant Control. To combat financial crime as part of the definition of UBOs, legal entity ownership has to be traced back to the natural persons who ultimately own or control the legal entity.

To be effective in preventing financial crime, Companies House must be properly resourced and use the latest technology to assist it in identifying companies formed for economic crime purposes. Reform of corporate entities and LLPs should not just be a matter for action by Companies House. Other government agencies must play their part – e.g. HMRC and other supervisors as well as, for example, the ICO (by acknowledging that there are appropriate inroads into data protection where criminal activity can be prevented). Cross checking with other government agencies should be facilitated. There should be a general legal duty to report discrepancies to Companies House. It may be that Companies House itself needs to be designated as an AML supervisor.

It is essential that Companies House becomes a proactive entity which makes it difficult and risky for bad actors to lie. The risk is as Chris Taggart “the bill is a better horse and cart and the criminals are driving round in fast cars”. If the business plan of a new LLP or company cannot cope with increased fees and applying ID to partners and directors, then Companies House must question whether it should be registered. The registrar needs duties not just

powers and the registrar should recognise red flags and query filings accordingly. We agree with Chris Taggart that Companies House needs to be the authoritative statement of record i.e. a definitive source of that status of a Company and those associated with it. It is also important that there is transparency on shareholders - a unique identifier for each real person associated with a company should be retained.

As Graham Barrow pointed out, criminals use networks of companies and leave Company DNA behind them. It is now possible using data analytics to extract the indicators of actual and potential criminal activity within historical records. Fake companies may be set up to imitate existing companies and use real identities without permission.

There should be a minimum age for PSCs and please also address the situation where the statement of capital is clearly, on the face of it, false. We consider that some friction in the opening of a company may not be negative and companies should not be registered until the requirements are met. Equally there should be service standards so that people can hold Companies house to account if they do not meet service levels.

We think a cap on the number of directorships a person can hold should be introduced and a system to apply if there are to be more than the specified number in exceptional cases. A large number of Company directorships certainly has to be a red flag for Companies House. The same should apply when multiple companies are registered at the same address.

However, in terms of capping the number of companies at any given address, while this may be feasible, Company formation agents may be an exception and should be flagged as such and again they should be properly and actively AML regulated and supervised.

Overall, we consider that the goal of anti-financial crime laws should be to make life hard for bad people without making life harder for good people. A great business environment can be enabled by making sure that a person's ID is transparent and, for example, people can see if a person has been involved as a director in several companies which have become insolvent. We want to be able to access historic data going back say 20 years as we know there has been a pattern of Corporates appearing and disappearing and being resurrected – so called “phoenix companies”.

There are private companies which can look at clusters of red flags – which taken together can indicate significant activity around Company formation by serious and organised crime. Companies House should engage with such technology. The Bill is trying to stop criminals registering a Company using details of a person without them being involved in that Company. However, the Bill should not permit legitimate directors or PSCs to be removed.

ID and V of DIRECTORS

There are some flaws in the proposed model, for example, Companies House should only outsource ID checks to those third-party professionals that are properly regulated under AML legislation and meet appropriate standards. Also, those third-party professionals should confirm they have taken all steps to ensure they have directly verified the ID and not relied on other third parties themselves. Furthermore, it may be that some ID service providers need to be brought within the scope of AML legislation.

SLAPPS AND COST LIMITATIONS

Anti SLAPP legislation was proposed in July this year and it appears to have stalled. It is crucial that these laws are passed and they must toughen the criteria for claimants to prove they have a legitimate claim. These measures are important to protect those who expose wrongdoing and act in the public interest. While we do not want to see this Bill delayed, we do consider SLAPPS to be an issue and that preventing SLAPPS will help prevent financial crime.

We believe that several government agencies such as the NCA and SFO and AML supervisors are concerned about prosecuting those who commit financial crime because they have no budget for the costs they would incur if they lost. In some instances, this prevents them even commencing action when there would be the chance to uncover more

information by using the legal process of discovery. In the US if Dept of Justice wins they keep the proceeds. One major case win could fund the entire prosecution case. In the UK the enforcement authorities seem to be fighting with metaphorically one hand tied behind their back and the current lack of enforcement makes a nonsense of any sort of deterrent or punishment as criminals know they will not suffer any consequences of their wrongdoing.

DATA SHARING

The PA welcomes measures to increase Information sharing which is key pillar to the prevention of financial crime. Improving data sharing between Financial Institutions, between government bodies and between the public and private sector is critical. Up to now, many FIs have felt too worried about civil liability to share information. At the Payments Association we especially want data sharing solutions which help all financial institutions as smaller payments companies are often the target of criminal activity and they should not be so disadvantaged. Improved data sharing will also give the opportunity for smaller payment companies to demonstrate compliance transparency and evidence that they meet compliance requirements by sharing the compliance data with regulatory authorities and banking providers. Companies should compete on the value of the services they offer and not on whether they prevent financial crime.

There is currently a failure to capitalise on the proven extensive investigative abilities which exist in both the public and private sector and the data which is uncovered by them. The government needs to find a way to facilitate the use of technology to enable secure data sharing either by a central body or bilaterally.

The government needs also to align with other regulatory authorities such as the FCA and HMRC to ensure that data sharing requirements are clear, and consistent to assist with the demonstration of compliance requirements within the financial industry and also across jurisdictions.

The UK has been a global leader in forming anti financial crime collaborative bodies such as the JMLIT. As Helena Wood stated in her oral evidence, such initiatives are now being copied at speed and scale in other jurisdictions. However these other jurisdictions are now moving from simple data sharing to collaborative data analytics (see for example initiatives in Holland by multiple banks <https://tmnl.nl/summary-eng/> and from MAS in Singapore <https://www.mas.gov.sg/news/media-releases/2022/additional-measures-to-strengthen-the-security-of-digital-banking>). The Bill's provisions will increase data sharing but they don't keep pace with global technological opportunities such as exploiting big data analytics.

CRYPTOASSETS

*“The Bill will provide **additional powers to law enforcement so they are able to seize and recover cryptoassets more quickly and easily** where those assets amount to the proceeds of crime or are associated with illicit activity such as money laundering, fraud or ransomware attacks. The Bill will principally amend both criminal confiscation powers in Parts 2, 3 and 4 of the Proceeds of Crime Act 2002 (POCA) and civil recovery powers in Part 5 of POCA to enable enforcement agencies to tackle criminal use of cryptoassets more effectively.”*

Whilst The Payments Association believes that this insertion is reasonable, it all depends on the implementation and interpretation of this provision. So “*where those assets amount to the proceeds of crime or associated...*” – as determined by a court of law / judgement? We believe that this section should specify this. In addition, it would be sensible if the provision covered freezing not just seizing of assets. So, if there is a court case or investigation after an allegation or ML or fraud relating to crypto, then such assets can be frozen (e.g. ordered to an exchange) under a warrant just like money in a bank pending outcome of trial.

The PA welcomes HMT's efforts to tackle cryptoasset-related financial crime through the Bill. These efforts are of critical importance for the long-term sustainability of the cryptoasset sector.

HMT has demonstrated an exceptional understanding of the relevant cryptoasset technologies in its drafting of the Bill, we have identified several points that may require further consideration.

Destruction of cryptoassets

The Bill empowers courts to order the "destruction" of cryptoassets in certain circumstances. We would note that, it may not be technologically possible to destroy certain cryptoassets (e.g. Bitcoin) such that alternatives means of disposal may need to be specified e.g. transferring the cryptoassets to a wallet in which they will be indefinitely frozen. Further guidance on when and how this power should be exercised may be helpful on this issue and in particular HMT may wish to consider the potential impact on the wider market e.g. deflationary effects of destroying cryptoassets.

Second, we understand that under the Bill an officer may require cryptoassets and/or cryptoasset-related items to be produced in a visible and legible form which can be taken away. This may not be possible in relation to certain cryptoassets. HMT should also consider whether this could give rise to any unintended data-protection risks.

Ownership of cryptoassets

The Bill provides for the return of cryptoassets to their "true owner" in certain scenarios. However, we would note that it is difficult to identify the owner of certain cryptoassets from both a legal and technological perspective especially where a third party such as an exchange or custodian / wallet provider is involved. This remains something of a legal grey area and case law on the ownership of cryptoassets continues to develop. The recent insolvency of FTX has also shown that it is not always clear how title / ownership to cryptoassets is recorded or can be demonstrated by creditors especially where intermediaries such as exchanges are involved. We would welcome further guidance on this issue.

Valuation

We welcome the Bill's introduction of new powers related to the seizure of cryptoassets. We note these powers often require the relevant authorities to determine the value of seized cryptoassets e.g. when disposing of or destroying seized cryptoassets. However, it is not clear how cryptoassets should be valued in those situations. As such, we encourage HMT to provide further guidance on how and when seized cryptoassets should be valued and who should bear the risk of market fluctuations.

Definitions

Under section 67ZB(5) and section 84A(5) of POCA 2002 (as amended by the Bill), the Secretary of State is empowered to amend certain cryptoasset-related definitions. We support HMT's efforts to construct a fluid framework capable of adapting to unforeseen developments in the sector. However, this power could allow the Secretary of State to amend certain cryptoasset-related definitions so they are inconsistent with equivalent definitions elsewhere. To prevent such a scenario, HMT may wish to consider a mechanism for ensuring cryptoasset definitions across different legislation remain consistent so as to avoid the potential for regulatory arbitrage or legal uncertainty.

Separately, we note the Bill's "cryptoassets" definition is drafted broadly. We support this dynamic approach. However, it appears the proposed definition could capture certain traditional financial instruments (e.g. derivatives that utilise DLT) and bring such instruments within scope of the Bill's cryptoasset-related provisions. If this was HMT's intention, then it may wish to clarify this in the Bill. If this was not HMT's intention then it may wish to expressly exclude traditional financial instruments from the "cryptoassets" definition.

AMENDMENT TO OVERSEAS REGISTER

We understand that Part 3 of the Bill would amend the Economic Crime (Transparency and Enforcement) Act 2022 to (i) maintain consistency with changes to the Companies Act 2006 made by this Bill; and (ii) make minor and technical changes. We welcome these amendments.

IMPROVEMENTS TO LAW ENFORCEMENT

We welcome these provisions.

About The Payments Association

The Payments Association (previously the Emerging Payments Association, or EPA) is a community for all companies in payments, whatever their size, capability, location or regulatory status. Its purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all. It works closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the PSR, Pay.UK, UK Finance and Innovate Finance.

Through its comprehensive programme of activities and with guidance from an independent Advisory Board of leading payments CEOs, The Payments Association facilitates the connections and builds the bridges that join the ecosystem together and make it stronger. These activities include a programme of monthly digital and face-to-face events including an annual conference, PAY360, The PAY360 Awards dinner, CEO round tables and training activities. The Payments Association also runs six stakeholder working project groups covering financial inclusion, regulation, financial crime, cross-border payments, open banking and digital currencies. The volunteers in these groups represent the collective views of the industry and work together to ensure the big problems facing the industry are addressed effectively. The association also conducts original research which is made available to members and the authorities. These include monthly whitepapers, insightful interviews, and tips from the industry's most successful CEOs.

See www.thepaymentsassociation.org for more information. Contact malik.smith@thepaymentsassociation.org for assistance.