Home Office Impact Assessment

Title: Information sharing between regulated entities (Economic Crime and Corporate Transparency Bill) **IA No:** HO0403 **RPC Reference No:** **Other departments or agencies:**	**Date**: 13 January 2023 **Stage:** FINAL **Intervention:** Domestic **Measure:** Primary Legislation **Enquiries:** Tom Bell tom.bell38@homeoffice.gov.uk
RPC Opinion: Not Applicable	**Business Impact Target:** Non qualifying provision

Cost of Preferred (or more likely) Option (in 2022/23 prices)					
Net Present Social Value NPSV (£m)	238.1	**Business Net Present Value BNPV (£m)**	0.0	**Net cost to business per year EANDCB (£m)**	0.0

What is the problem under consideration? Why is government intervention necessary?

Businesses in the anti-money laundering regulated sector are constrained in their ability to share information with each other about economic crime, due to a duty of confidentiality they owe to their customers, as well as risk of potential vexatious and/or unmeritorious litigations. As a result, a single bank trying to determine whether economic crime is occurring, can usually only see their own customer data in what is a larger, more complicated network, making it difficult to determine a transaction's legitimacy. Criminals whose relationship is terminated with one bank can open an account with another institution. The Government has to intervene to remove the duty of confidentiality a business owes when it shares information for the purpose of preventing and detecting economic crime.

What are the strategic and policy objectives and the intended effects?

The strategic objective of the proposal is to reduce crime, to increase UK prosperity and enhance security. The policy objectives are to make it easier for businesses to: a) identify whether a transaction is legitimate, and b) prevent criminals from re-entering the system by allowing businesses to share information with each other. To enable this, a disapplication of civil liability for all forms of civil liability owed to the person to whom the disclosed information relates, other than those UK GDPR arising under data protection legislation, when a specified business shares customer information with another specified business for the purposes of preventing and detecting economic crime is proposed.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

Option 1: 'Do-nothing', whereby there would be no government intervention to facilitate information sharing between financial and credit institutions where they have a suspicion of economic crime.

Option 2: Introduce permissive legislation to enable specified businesses to share information between themselves to tackle 'economic crimes'. Economic crime in this legislation includes: money-laundering, fraud, corruption, sanction-evasion and counter-terrorist financing. **This is the Government's preferred option** and it meets the Government's objectives.

Main assumptions/sensitivities and economic/analytical risks	**Discount rate (%)**	3.5

Data on Suspicious Activity Reports (SARs) volumes from 2016-20 is used to estimate growth rates for future SARs of between 3 and 20 per cent year-on-year and is highly uncertain. This is used to estimate expected SARs volumes. Future growth may not follow the same trends and SARs volumes could grow more or less than this range. Firms are assumed to use a privately funded third-party platform to share information and the platform will take time to reach the estimated level of utilisation (but the approach to information sharing will not be prescribed). A significant number of assumptions and data rely on responses from stakeholders in workshops.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** October 2026

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister: Tom Tugendhat Date: 23/01/2023

Summary: Analysis & Evidence Policy Option 2

Description: Information sharing between regulated entities (Economic Crime Bill 2022)

FULL ECONOMIC ASSESSMENT

Year(s):	Price Base	2021/22	PV Base	2022/23	Appraisal	10	Transition	1
Estimate of Net Present Social Value NPSV (£m)						**Estimate of BNPV (£m)**		
Low:	9.4	**High:**	1,675.2	**Best:**	**238.1**	**Best BNPV**	**0.0**	

COSTS, £m	**Transition** Constant Price	**Ongoing** Present Value	**Total** Present Value	**Average/year** Constant Price	**To Business** Present Value
Low	7.2	79.9	**87.1**	10.1	87.1
High	46.4	114.0	**160.3**	18.0	160.3
Best Estimate	17.4	88.1	**105.5**	**12.1**	**105.5**

Description and scale of key monetised costs by 'main affected groups'

Set-up, familiarisation and staff training costs are estimated to be **£7.2 to £46.4 million**, with a central estimate of **£17.4 million** (2021/22 prices) in year 1 only. Ongoing costs are estimated to be **£79.9 to £114.0 million (PV)**, with a central estimate of **£88.1 million (PV)** over 10 years. Total costs are estimated to be **£87.1 to £160.3 million (PV)**, with a central estimate of **£105.5 million (PV)** over 10 years.

Other key non-monetised costs by 'main affected groups'

There may be some additional administration costs.

BENEFITS, £m	**Transition** Constant Price	**Ongoing** Present Value	**Total** Present Value	**Average/year** Constant Price	**To Business** Present Value
Low	0.0	96.4	**96.4**	11.1	79.1
High	0.0	1,835.5	**1,835.5**	216.2	131.8
Best Estimate	**0.0**	343.6	**343.6**	**40.1**	**105.4**

Description and scale of key monetised benefits by 'main affected groups'

Total ongoing benefits are estimated to be **£96.4 to £1,835.5 million (PV)**, with a central estimate of **£343.6 million (PV)** over 10 years. These are driven by the benefits of crimes prevented. The considerable degree of uncertainty in SARs volume trajectories is reflected in the estimated benefits, more so in the high scenario estimates.

Other key non-monetised benefits by 'main affected groups'

Increased information sharing is expected to improve the efficiency of onboarding, due diligence and remediation processes for regulated entities, due to improved ability to assess risk. Trust and confidence in the regulated sector could be increased with a reduction in money laundering facilitated due to these policies. Non-monetised benefits are significant (see Evidence Base).

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:					
Cost, £m	0.0	**Benefit, £m**	0.0	**Net, £m**	**0.0**
Score for Business Impact Target (qualifying provisions only) £m:					0.0

Is this measure likely to impact on trade and investment?					N				
Are any of these organisations in scope?	**Micro**	Y	**Small**	Y	**Medium**	Y	**Large**	Y	
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)	Traded:	N/A	Non-Traded:	N/A					

PEOPLE AND SPECIFIC IMPACTS ASSESSMENT (Option 2)

Are all relevant Specific Impacts included?	Y	**Are there any impacts on particular groups?**	N

Evidence Base (for summary sheets)

A. Strategic Overview

A.1 Strategic Objective

1. Criminals continue to be relentless in their pursuit of financial gain and Government's collaborative efforts must match and exceed their relentlessness.

2. The strategic objective is to contribute to reduce crime, and to increase UK prosperity and enhance security.

3. This intervention is one of several interventions considered for Reforming Economic Crime Legislation. Government has listened to colleagues in law enforcement agencies (LEAs), the private sector and elsewhere and has heard the case for further legislative reform on economic crime, particularly to: enable effective information sharing; continue to improve the overall response to money laundering (informed by the recent Law Commission Review[1] on aspects of the Suspicious Activity Reporting (SARs) regime and its ongoing review of the confiscation regime), and to strengthen the Government's ability to recover the proceeds of crime.

4. The measures considered in this impact assessment (IA) are aimed at enabling better information sharing between businesses (private to private information sharing), in order to better detect and prevent money laundering. This proposal would allow businesses, for example, banks, to take a more informed and proactive role in preventing and detecting economic crime, for instance by identifying networks operating across different institutions and stopping 'account shopping' whereby accounts are typically closed in one bank, with new accounts opened at a different bank by the criminal shortly after.

A.2 Background

5. Large amounts of financial data flow through the UK every hour. The overwhelming majority of this data relates to legitimate activity. However, a small proportion involves criminal activity. At present, businesses are constrained in their ability to share information between themselves (private to private information sharing) which would help them better detect and prevent this kind of criminal activity. These constraints arise due to concerns over client contract or confidentiality duties and data protection law.

6. This means that a bank concerned that one of its customers is engaged in, for instance, money laundering, is only able to see its own data when conducting an investigation. This is despite the fact that economic crimes such as money laundering are complex and take place across multiple bank accounts hosted by separate businesses.

7. Whilst provisions exist to share information via the UK Financial Intelligence Unit (UKFIU) or with UKFIU involvement, the number of SARs submitted each year (approximately 742,300 in 2020/21) means that the FIU is only able to prioritise the highest value cases. As a consequence, many opportunities for the private sector to prevent and disrupt economic crime at an early stage may be missed.

8. The Government intends to make it easier for certain businesses to share information with each other. To enable this, it is proposed that civil liability for all forms of civil liability owed to the person to whom the disclosed information relates, other than those arising under data protection legislation, UK GDPR should be disapplied when a business shares customer information with another for the purposes of preventing and detecting economic crime.

9. Civil liability for certain institutions sharing information is already disapplied under section 339ZF of Proceeds of Crime Act 2002 (POCA 2002), where an institution shares customer information for the

[1] The Law Commission final report on the UK SARs regime | Regulation Tomorrow

purposes of making a disclosure in compliance or intended compliance with section 339ZB. It is proposed that new legislation would make provisions along similar lines for businesses who are sharing information for the purposes outlined in the proposed legislation, protecting firms against civil liabilities, for instance defamation, discrimination, or negligence claims.

10. The proposed legislation would disapply any obligation of confidence owed by the institution sharing the information, where the information is shared for the purpose of preventing or detecting economic crime. Unlike section 339ZF of POCA 2002, the proposal would allow businesses to share information amongst themselves without having to involve law enforcement.

11. The proposed legislation is anticipated to have benefits to businesses, such as improving their ability to assess risk and avoiding costly onboarding, due diligence and remediation processes as a result. This improved ability to assess risk may also increase trust and confidence in the regulated sector.

    a. The onboarding of problem customers can be expensive for credit and financial institutions. These costs include the initial onboarding checks and subsequent due diligence on high-risk customers. During 2019/20 761,437 customers were exited[2] from all lines of business for financial crime reasons[3]. These are customers that firms could have potentially avoided onboarding and avoided the onboarding costs. Using an average unit cost[4] of £3.50 suggests it cost firms approximately **£2.7 million per year** to onboard customers that were subsequently exited for financial crime reasons. Assuming the level of customers exited yearly is unchanged[5], the costs to firms is estimated at **£23 million (PV)[6]** over 10 years. There is a high degree of uncertainty with this estimate as the data from the Financial Conduct Authority (FCA) was reliant on a single case of a bank reporting onboarding expenses. The estimated costs could be an under-estimate or over-estimate, but it suggests it is a costly problem for businesses.
    b. In addition to onboarding costs, high risk customers are to be reported by businesses in compliance with Regulation 33(1)(a) of the Money Laundering Regulations (MLRs) and subject to enhanced customer due diligence measures. Enhanced customer due diligence is costly to firms, if a potential customer is not onboarded by a firm then they are not subjected to the due diligence, and the firm could avoid these costs. According to data from FCA, there were 735,967 high-risk customers reported for the period 2019/20[7]. Using an average unit cost[8] of £25 to perform due diligence suggests it cost firms approximately **£18.4 million in 2019/2020** to perform these checks. Using the growth trend of available data on high-risk customers to estimate 10 years volume of due diligence[9], the costs to be business is estimated at approximately **£86 million (PV)** over 10 years. There is a high degree of uncertainty with this estimate, as the data from the FCA was reliant on a single case of a bank reporting their level of due diligence expenses. The estimated costs could be an under-estimation or over-estimation, but it suggests it is a costly problem for businesses.
    c. These onboarding and due diligence costs to firms informs the rationale that firms will chose to act by making use of the information sharing legislation. The estimated costs to set-up and run an IT platform that enables information sharing that could help screen out potential problem customers seems a more cost-effective solution than the current system.

[2] According to the FCA :"This covers any customers or clients with whom the firm ceased to do business where financial crime or criminal behaviour by a customer or client with a financial element was the principle driver behind the decision.

[3] Financial Crime: analysis of firms' 2017-2020 REP-CRIM data | FCA

[4] Drivers & Impacts of Derisking (fca.org.uk) (p.66-67): Calculated by taking an average of £1 per customer for individuals and £6 for businesses. This cost relates to screening and risk assessing customers but exclude the front-line costs of the initial on-boarding, so the cost captures a fraction of total costs. Also, 0.2% of customers are referred for more detailed risk assessments costing £10-40 each, these haven't been included in the unit costs given how small the fraction is.

[5] Data unavailability to estimate growth trends means this assumption is necessary.

[6] PV = present values, that is the total over 10 years has been discounted by 3.5 per cent (the social discount rate).

[7] Financial Crime: analysis of firms' 2017-2020 REP-CRIM data | FCA

[8] Drivers & Impacts of Derisking (fca.org.uk) (p.66-67). Calculated by taking an average of cost of a more detailed risk assessment which is £10-40.

[9] There were 1,047,338, 797,416, and 735,967 high-risk customers reported in reporting periods 2017/18, 2018/19 and 2019/20 respectively.

What type of information can be shared and by whom?

12. Customer information would only be shared for the purposes of preventing and detecting the offences specified in the proposed legislation. The sharing of customer information for reasons outside of this purpose would not be subject to the proposed disapplication, meaning businesses would still be liable.

13. Based on this clearly defined purpose, the type of information that can be shared is that which would, or may, assist in enabling the recipient either to:

    a. Determine whether there are reasons to doubt the veracity of documents or information obtained for the purposes of identifying, or verifying the identity of, a new or existing customer.

    b. Determine whether it is appropriate to take customer due diligence measures in relation to an existing customer.

    c. Assess whether there is a high risk of economic crime associated with a particular case or customer, and the extent of the measures which should be taken to manage or mitigate that risk.

A.3 Groups affected

14. Those businesses to whom the power applies will be affected. This will be limited to the Anti-Money Laundering (AML) regulated sector for direct (peer to peer) information sharing, and large insolvency practitioners, auditors, tax advisors, large accountancy and law firms (defined as those with UK revenues above £36m) as well as the financial sector, including crypto exchanges and wallet providers, for indirect (third party) information sharing with the power to extend the provision to other sectors provided for in secondary legislation. At present, the AML regulated entities under the POCA 2002) must submit a SAR when there is suspicion about potential criminal activity, but the new information sharing legislation would add an additional burden on institutions who chose to use the provision to share information (the provision will be voluntary). If the method of information sharing is through a third-party platform, the cost for this platform is likely to be borne by the private sector via a user-pays subscription model, in the same way as the National Fraud Database currently hosted by Cifas.

15. By signing up to a platform, businesses will be more easily able to comply with their obligations under the MLRs, including the obligations to put policies and procedures in place in order to prevent money laundering and terrorist financing; apply customer due diligence measures to verify the identity of their customers; and conduct regular risk assessments of their business. Compliance with the MLRs is overseen by a range of different supervisors, including the FCA for financial services and failure to comply with the MLRs can result in significant fines or criminal penalties. Given the costs involved of signing up to a third-party platform, it is likely (based on consultation with the sector) that the majority of initial users are likely to come from large businesses (over 100 employees) such as the major retail and investment banks.

16. Businesses are also expected to benefit from the increased information sharing, through increased efficiency of onboarding, due diligence and remediation processes. Although the measures are permissive, meaning that businesses are not compelled to take part in private information sharing, evidence suggests businesses have an incentive to act (discussed in the Background section).

17. Individuals may also be affected. There is a risk that an already excluded customer could find themselves excluded from a wider range of products and services within a sector. This impact is expected to be mitigated by ensuring that the stipulations of the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR 2018) remain in full. This includes the limitations it imposes around accuracy, use and storage of data, oversight by the Information Commissioner's Office (ICO) (and other relevant supervisors such as the FCA for the financial sector), and appropriate and effective governance and robust frameworks for appeal against financial exclusion under the authority of the Financial Ombudsman. In the majority of cases, an individual excluded from multiple institutions is still likely to have the right to a Basic Bank Account

(BBA) under the Payments Accounts Regulations 2015 (PAR 2015) (see 'Risks' section for more detail).

A.4 Consultation

18. This IA accompanies the Economic Crime and Corporate Transparency Bill.
19. To enable information sharing to take place, the Government issued a targeted consultation paper to consult on introducing private-to-private information sharing for regulated sector entities for the purposes of preventing and detecting money laundering.
20. The targeted consultation sought views from the main stakeholders in the AML regulated sector and wider organisations that are impacted by economic crime. The targeted consultation paper set out 35 questions on measures covering AML, cryptoassets and Unexplained Wealth Orders (UWOs). It was shared with over 100 organisations. Written responses were received from 44 organisations (44%) and approximately 90 per cent of respondents were from within the AML regulated sector.
21. Feedback from the targeted consultation led to the decision to limit the users of information sharing measures, but to cover a broader range of crimes. The banking and financial sector noted that the proposed powers, which confined information sharing solely in relation to money laundering, were too narrow to fully realise the potential benefits of this power. Although a majority of respondents agreed in principle with the removal of barriers to sharing appropriate information to tackle money laundering, accountancy firms noted that the proposals seemed to target primarily financial institutions and were unsure whether the proposals would add value to their sector due to the fact that many accountants and lawyers run small practices (less than five people) and so the costs to the businesses and additional burdens in terms of data security and storage were unlikely to outweigh the benefits. The consultation informed the decision to initially limit information sharing measures to credit and financial institutions, rather than the whole regulated sector, and to expand the measures to cover economic crime (including money-laundering, fraud, bribery, sanction-evasion and counter-terrorist financing), as opposed to money laundering only.
22. Following the targeted consultation exercise, the accounting sector requested that indirect sharing be expanded to accountancy firms whose size and data controls mean that they are able to adequately manage the risks around data misuse and access. Following the accountancy sector approach, the legal sector also made similar requests. Based on their feedback, the indirect sharing measures were expanded to include large accountancy and legal firms using the definition of large firms under the Economic Crime Levy.

B. Rationale for intervention

Problem under consideration

23. Businesses are constrained in their ability to share information with each other about economic crime due to a duty of confidentiality that they owe to their customers, as well as risk of potential vexatious and/or unmeritorious litigations. A bank trying to determine whether economic crime is occurring, can usually only see their own customer data in what is a larger and more complicated network, making it difficult to determine whether a transaction is legitimate. Criminals whose relationship is terminated with one bank can open an account with another institution without the new institution knowing about the concerns of the former account provider.
24. By allowing businesses to engage in private-to-private information sharing they will have better information with which to address criminal financial activities. It will allow them to avoid onboarding criminals who have already been refused a service elsewhere due to suspicion of economic crime and help businesses to spot criminal networks across different providers. The incentive for businesses to engage in information sharing is partially the avoidance of costly onboarding processes, expanded on in the Background section, but there are also further benefits to business

such as an enhanced ability to assess risk, leading to more efficient and effective due diligence and remediation, and increased trust and confidence in the sector.

C. Policy objective

25. The policy objective is to:

    a. Enable specified businesses to share customer information with one another for the purposes of preventing and detecting economic crime. This will:

        a.1 Help to prevent the displacement of crime, where criminals who are exited or refused a service from one institution are able to exploit the system through other service providers.

        a.2 Help businesses spot criminal networks across different providers. At present they can only see their own data in a wider web of transactions.

        a.3 Improve the accuracy of SARs into law enforcement.

    b. Increase transparency, due diligence and remediation for the regulated sector. At present, there is not a facility that enables regulated sector organisations to alert each other to suspicious activity, meaning that regulated entities incur unnecessary remediation and onboarding costs.

    c. Improve trust and confidence in the regulated sector if there is a reduction in economic crime facilitated as a result of these policies.

D. Options considered and implementation

Option 1: 'Do Nothing'

26. **Option 1** would entail no further government intervention to facilitate information sharing between regulated entities. Civil liability for certain institutions sharing information is already disapplied under section 339ZF of POCA 2002, where an institution shares customer information for the purposes of making a disclosure in compliance or intended compliance with section 339ZB of POCA 2002. Under the **Option 1**, this would not be extended to disapply any obligation of confidence where information is shared for the purpose of preventing or detecting economic crime. It does not meet the Government's objectives.

Option 2:

27. Legislation to disapply all forms of civil liability (other than under the UK GDPR 2018) owed by the institution sharing the information, where the information is shared for the purpose of preventing or detecting 'economic crimes'. **This is the Governments preferred option** and it meets the Government's objectives.

    - **Option 2** requires primary legislation to enable specific businesses to share information with one another where they have suspicion of 'economic crime' without the need to involve law enforcement. The legislation would disapply any obligation of confidence owed by the institution sharing the information, where the information is shared for the purpose of preventing or detecting economic crime. The legislation would also protect firms against all other forms of civil liability owed to the person to whom the disclosed information relates, other than those arising under data protection legislation when they are sharing information for the purposes of preventing, detecting and investigating economic crime.
    - There is currently no statutory definition of economic crime, nor does this legislation seek to define one. Instead, the scope of offences this legislation will cover will include money-laundering, fraud, corruption, market abuse, sanction-evasion and counter terrorist financing.
    - The method of information sharing will not be prescribed by government but could be achieved through the use of a third-party platform to facilitate sharing.

- To begin with, businesses able to rely on the exclusion of liability will be limited to the AML regulated sector for direct information sharing, and large insolvency practitioners, auditors, tax advisors, large accountancy and law firms (defined as those with UK revenues above £36m) as well as the financial sector, including crypto exchanges and wallet providers, for indirect information sharing, with the power to extend the provision to other sectors provided for in secondary legislation. Limiting the provision to these businesses would be the most proportionate and provide the greatest protection and oversight.
- Using guidance instead of legislation has been explored, but this was not deemed to have legal force.

E. Appraisal

General assumptions and data

- The appraisal period for measuring the impacts of the proposed changes is 10 years and starts in 2022/23, so 10-year estimates are in present values (PV) and 2022/23 prices.
- A 3.5 per cent annual social discount rate is used. [10]
- Annual costs and benefits are in 2021/22 prices.
- All costs and benefits are relative to **Option 1**: 'Do-nothing'.
- The specific approach to information sharing will not be prescribed by government, but it is assumed that firms will use a privately funded third party platform to facilitate information sharing[11].
- As the legislation is permissive it relies on businesses choosing to take action to facilitate information sharing. If businesses perceive that the costs to information sharing outweigh the benefits and do not decide to share information, there will be no benefits. The estimates of benefits are highly uncertain and are reliant on businesses choosing to take action. Evidence indicate businesses have incentive to act, see paragraph 11.
- It is assumed that a third-party platform will take time to reach the estimated level of utilisation, with 50 per cent of benefits beginning in Year 1 and 100 per cent of benefits from Year 2 onwards.
- All calculations using median hourly wages are taken from the Annual Survey of Hours and Earnings (ASHE) 2020, Table 14.5)[12]. The 2020 figures have been used as a more realistic cost estimate, as the figures from 2021 appear to be impacted by the drop in wages and employment as a result of the pandemic and may under-estimate costs. The 2020 values, once inflated to price year 2021/22, are closely in line with the ASHE 2019 data (data as pre-pandemic).
- The appraisal here relies on the number of SARs reports[13], which cover only suspicions related to money laundering and terrorist financing. A reduction in bribery, corruption and sanctions evasion crimes has not been modelled due to a lack of data. It is assumed that these cases will make up a very small proportion of the total cases reported via the information sharing

[10] The Green Book (publishing.service.gov.uk)

[11] It is assumed that a third-party platform similar to Cifas (a platform for sharing information about fraud) is the most likely method of information sharing between businesses, based on extensive feedback and engagement with the financial sector. A pilot scheme is currently underway to test the viability of such a platform for sharing information about economic crime more widely, where participants are able to share information using Cifas.

[12]https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

[13] Suspicious Activity Reports (SARs) are made by financial institutions and other professionals such as solicitors and accountants, and they alert law enforcement to potential instances of money laundering or terrorist financing. Suspicious Activity Reports - National Crime Agency

measures and should not significantly impact the results. Although the proposed information sharing measures will also allow institutions to share information related to fraud, there is an existing platform for regulated sector entities to share information where there is a suspicion of fraud, called Cifas. Inclusion of fraud in the proposed information sharing measures is predominantly for completeness and will only provide additional cover to businesses for the information sharing already taking place via Cifas. These measures are not expected to capture additional fraud cases, therefore have not been modelled.

- Information sharing will be available to the AML regulated sector for direct information sharing, and large insolvency practitioners, auditors, tax advisors, large accountancy, large law firms and the financial sector, including crypto exchanges and wallet providers, for indirect information sharing, however it is anticipated that deposit taking bodies and payment institutions will be the majority users. The majority of the costs and benefits relate to this sector.

Inputs

28. Many of the cost and benefit estimations relies on data from a stakeholder workshop with the regulated sector facilitated by Deloitte. The workshop had participants from 14 different firms from the regulated sector. These firms came from a variety of different regulated subsectors, though there were no representatives from financial technology (fintech) firms. Deloitte engaged externally with a fintech firm to gather relevant evidence. The inputs used in these estimates include the proportion of SARs related to a customer exit or refusal, crime displacement[14], usage of the third-party platform (for both submitting and checking data) and the time taken to submit information to the platform (which is based on the estimated time taken to submit a SAR).

29. The number of SARs reports per year is from the National Crime Agency (NCA) Annual Report 2020[15]. The NCA data shows that SARs volumes have been increasing year on year. Table 1 shows the number of SARs reported each year since 2016/17 and the respective percentage increases. Based on the most recent four years of data, SARs volumes have been increased at between 3 and 30 per cent each year, with an average of 16 per cent each year. A low, central and high range of 3, 11 and 30 per cent has been applied for the percentage increase in SARs reports expected per year. The uncertainty around factors driving SARs volume growth trends informs the additional assumption that the growth rate applies for the second and third year in the modelled period before levelling off.

Table 1, Historical volume and percentage increase in SARs per year, 2016/17-19/20.

Year	Number of SARs	Percentage increase (%)
2016-17	423,304	-
2017-18	463,938	10
2018-19	478,437	3
2019-20	573,085	20
2022-21	742,317	30
Average percentage increase		**16**

Source: NCA SARs data 2016-2021.

30. A conversion ratio of reports (that is, information shared) to crime events prevented has been used, based on proxy data from Cifas.

Appraisal

[14] The percentage of displacement refers to how many crimes are simply displaced to elsewhere in the system, not actually prevented. For example, a displacement percentage of 90 per cent means that 90 per cent of crimes are displaced, and just 10 per cent are actually prevented.

[15] file (nationalcrimeagency.gov.uk), file (nationalcrimeagency.gov.uk), file (nationalcrimeagency.gov.uk)

31. The estimated costs associated with the preferred option are familiarisation costs, set-up and running costs of using a third-party platform for information sharing (though the specific approach to information sharing will not be prescribed), and administrative/time costs associated with submitting information to the platform. The greater administrative costs are expected to be mitigated by efficiency gains in customer on-boarding processes expected as a result of these proposals.

32. The expected benefits are a reduction in economic crime and other predicate offences, such as drug and other crime, improved ability of the regulated sector to assess risk, improved efficiency of customer on-boarding, due diligence and associated remediation, and greater trust and confidence in the regulated sector.

33. Benefits have been modelled based on the scenario where a deposit-taking or payment institution (as the anticipated majority user) has submitted a SAR and then taken action against a customer as a result of their suspicion, for example, exiting the customer or refusing a service. A SAR is submitted by a business to alert LEAs to potential instances of money laundering or terrorist financing, and SARs provide information and intelligence from the private sector that would otherwise not be visible to LEAs[16]. Under POCA 2002, a business in the regulated sector has a duty to submit a SAR when they have suspicions of money laundering. The threshold for suspicion is not defined in legislation but has been interpreted as "*more than a fanciful possibility*", making it a relatively low threshold. As a result, in most cases where a bank has got to the point where it would want to share information with another bank, it would also have met the suspicion threshold, and would thus be obliged to have submitted a SAR to the UKFIU. Whilst the proposed information sharing measure will allow for information to be shared under a broader range of scenarios, it has not been possible to model these scenarios due to a lack of data. It is possible that there will be greater benefits than those modelled, as firms will be allowed to share information under a broader range of scenarios, but the focus of this analysis will be on monetising scenarios for which there is robust data.

34. Where regulated entities can share information about a customer, they have suspicions about before they have submitted a SAR, or taken action against the customer, it has not been possible to estimate the number of eligible cases. However, regulated entities currently submit a significant amount of SARs (approximately 742,300 in 2020/21)[17], suggesting that they already act with a significant level of caution. Stakeholder engagement has confirmed that financial and credit institutions tend to be risk averse and would submit a SAR where they have any concerns about possible financial crime. Given this, and the low threshold for suspicion ('more than a fanciful possibility'), it is assumed that in the majority of cases where regulated entities have any suspicion of financial crime, a SAR will be submitted. The modelling here assumes that a regulated entity will only take the additional step of sharing customer information to a platform once they are confident about their suspicion, which in this case has been defined as taking action against a customer. This is because, if a regulated entity has not taken action against a customer, they may not see the need for sharing information to other entities.

35. Owing to uncertainty, low, central and high estimates are presented for the costs and benefits. These are developed from a range of values for expected percentage growth in SARs volumes, the proportion of SARs related to customer exit/refusals, expected usage of the third-party platform, and crime displacement.

36. Whilst the measure does not mandate information sharing between firms, nor specify the mechanism via which sharing must take place, the most likely scenario to arise following introduction of the measure (based on extensive feedback and engagement with the financial sector) is a privately funded third party platform for exchanging information on economic crime, similar to the Cifas hosted National Fraud Database.

[16] According to the NCA, some SARs provide immediate opportunities to stop crime and arrest offenders, others help uncover potential criminality that needs to be investigated, while others provide intelligence useful in the future, making them a good proxy for the new information sharing measures. www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

[17] Direct engagement with NCA.

COSTS

Set-up costs

Private familiarisation costs

37. It is assumed that all credit and financial sector firms (1,175), and 15 per cent of the remaining firms in the AML sector (7,474 of 49,825) read (in a L, C and H scenario) 600, 800 or 1,000 words on a screen or on paper to become familiar with the new legislation. This gives an estimate of 1.2, 3 and 8 minutes per person to become familiar with new legislation[18]. It is assumed that two, four and five people in each firm will need to become familiar with the new legislation[19]. Typically, time will be spent building an understanding of what the legislation means and its relationship with existing policies. The measures will apply to the AML regulated sector for direct information sharing, and large insolvency practitioners, auditors, tax advisors, large accountancy, large law firms and the financial sector, including crypto exchanges and wallet providers, for indirect information sharing, however it is anticipated that deposit taking bodies and payment institutions will be the majority users and therefore familiarisation costs will be higher for such firms. According to Business Population Estimates 2021, this represents around 1,175 firms ('Monetary intermediation' and 'Trusts, funds and similar financial entities', Table 7, Standard Industrial Classification (SIC) code 64.1 and 64.3 respectively)[20].

38. For all firms, time has been valued using data from the Annual Survey of Hours and Earnings (ASHE) 2020, Table 14.5a. The analysis uses a median wage figure for financial institution managers and directors (SOC code 1150) of £26.00 per hour[21], which is then uplifted by the non-wage share of costs of 22 per cent to reflect the marginal product of labour[22].

39. The values used to estimate the familiarisation costs are presented in Table 3 and given as:

Number of firms x number of readers in each firm x average familiarisation time x (median financial institution managers and directors wage x non-wage uplift of 22%)

40. The estimated cost lies in a range of **£0.01 and £0.18 million**, with a central estimate of **£0.06 million** in year 1 only (2021/22 prices). Business engagements during the targeted consultation did not indicate that any additional dissemination of information costs or training would be needed, so these costs are not included in the familiarisation costs to businesses.

Table 2, Familiarisation costs to business in year 1 only, £ million 2021/22 prices, 2022.

Estimate	Number of firms	No. readers per firm	No. words to read	Reading speed (wpm)	Average time (hrs)	Cost per hour (£)	Cost to business (£m)
Low	8,649	2	600	700	0.02	31.83	**0.01**
Central	8,649	4	800	400	0.05	31.83	**0.06**
High	8,649	5	1,000	200	0.13	31.83	**0.18**

Source: Business Population Estimates 2021, Assumption, readingsoft.com, ASHE 2020, Table 14.5a.
Note: wpm = words per minute.

Third party platform set up costs to business

[18] Based on readingsoft average of 200wpm with 60 per cent comprehension, slightly uplifted to allow for full comprehension Speed Reading Test Online (readingsoft.com)

[19] Number of readers in each firm is a weighted average that accounts for the size of firms in the business population. The assumption on the number of readers in each category of firm size differ. For micro firms, the number of readers is assumed to be two (low), three (central), and three (high). For small firms (two, three, and five respectively), medium firms (two, five, 10), and for large firms (five, 10, 20). Approximately 82 per cent of firms in the 'Monetary intermediation' and 'Trusts, funds and similar financial entities' are micro and small firms, which informs the overall low scenario assumption of two readers per firm.

[20] Note that this does not include sole proprietors, only firms who employ people Business population estimates 2021 - GOV.UK (www.gov.uk)

[21] Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics (ons.gov.uk)

[22] Non-wage cost is 17.9 per cent (from Eurostat), take 18/(100-18) = 18/82 = 22 per cent and uplift by this amount. https://ec.europa.eu/eurostat/databrowser/view/LC_LCI_LEV__custom_2052124/default/table?lang=en

41. The Government would not prescribe a mechanism to facilitate information sharing between regulated entities, but for the purposes of this analysis it is assumed that firms will use a privately funded third-party platform. There will be costs associated with implementing a third-party platform. It is assumed that there are three potential directions regulated entities could take. In the high scenario, it is assumed a bespoke system is developed. For the central scenario, an off-the-shelf platform is given a major amendment. And for the low scenario, minor amendments are made to an off-the-shelf platform.

42. For the bespoke option, proxy cost data from the SARs IT Transformation programme is used. The programme is being delivered by the NCA to replace the current ELMER database used for monitoring financial transactions and processing SARs raised by regulated entities, and as such, the costs are a suitable proxy at approximately £22 million[23]. The IT cost structure is assumed to follow the same as those used by the FCA to assess IT programmes of regulated entities. Since the FCA regulate entities that are impacted by legislation, their cost structure is an appropriate proxy (see Table 3)[24].

43. For the low and central scenario, adjustments are made to the bespoke option cost, for example, the design costs are expected to smaller when amendments are made to a system compared to developing a new bespoke system. The costs are halved in the central scenario, and further halved in the low scenario., Optimism bias was applied, at 25, 50, and 100 per cent for the low, central, and high scenario respectively.

Table 3, Third-party platform set-up costs to business, (£ million 2021/22 prices).

Element	Percentage of resource (%)	Low	Central	High
Business Analysis	10	0.6	1.1	2.2
Design	10	0.6	1.1	2.2
Programming/coding	55	3.1	6.2	12.3
Project Management	10	0.6	1.1	2.2
Testing	10	0.6	1.1	2.2
Senior Management	5	0.3	0.6	1.1
Sub-total		**5.6**	**11.2**	**22.4**
Optimism Bias		1.4	5.6	22.4
Total cost		**7.0**	**16.8**	**44.8**

Source: NCA, FCA.

44. Total third-party platform set-up costs are estimated in a range of **£7.0 to £44.8 million**, with a central estimate of **£16.8 million** (2021/22 prices). Given that the proposed measure is permissive, businesses are not obliged to act and set-up the IT platform, and as such this is classified as an indirect cost and not included in the BNPV or EANDCB.

Private training costs

45. There are expected to be some training costs for staff in financial and credit institutions to learn the processes around submitting information to the platform. It is anticipated that some staff in financial crime teams will be expected to participate in information sharing and would require training. A study by FCA states that there are 17,403 full-time equivalent staff in financial crime roles[25]. However, it is

[23] This does not include future development or support, this is the cost to deliver just the platform. The ongoing costs are captured in another section of the IA.

[24] How we analyse the costs and benefits of our policies (fca.org.uk), table A4. The table included proportion that equated to 110 per cent, which probably accounts for optimism bias. Since optimism bias is applied separately in this IA, the business analysis and design proportion are reduced by 5 per cent in this IA.

[25] Financial Crime: analysis of firms' 2017-2020 REP-CRIM data | FCA

not anticipated that all of these staff would have access to the platform, as it would hold personal customer information which may be sensitive.

46. The NCA uses a database called ELMER for monitoring financial transactions and processing SARs raised by regulated entities. Only about three per cent of police officers have access to the system[26]. Taking the ELMER database as a proxy and applying three per cent to the total number of people working in financial crime gives the high estimate of 550 people who are expected to have access to the information sharing platform and would need training. This figure is then halved for the central estimate and halved again for the low estimate.

47. The average cost to train staff is taken from research by the UK Commission for Employment and Skills, with the average amount spent by firms on training estimated to be approximately £2,550 per person trained[27] across twelve months. Given that this covers all training for an employee over the year, and not a specific training course like the sort probably required for the third-party platform, this is taken as the high estimate. The central and low estimates are set at 75 and 50 per cent of the high scenario.

48. The values used to estimate the training costs are presented in Table 4 and given as:

Number of employees expected to require training x average cost to train one member of staff

Table 4, Training costs to business in year 1 only, 2021/22 prices, 2022.

Estimate	No. people to be trained	Unit training cost (£)	Total training cost (£m)
Low	140	1,275	**0.2**
Central	275	1,910	**0.5**
High	550	2,550	**1.4**

Source: FCA, UKFIU engagement, Home Office Police Workforce data, UK Commission for Employment and Skills, 2021.

49. Total training costs are estimated in a range of **£0.2 to £1.4 million**, with a central estimate of **£0.5 million** (2021/22 prices) in year 1 only. Given that the proposed measure is permissive, businesses are not obliged to act and set-up the IT platform, and as such this is classified as an indirect cost and not included in the BNPV or EANDCB.

Ongoing costs

Administration cost to business of information sharing

50. There will be some costs related to the administrative burden for staff in regulated entities to share information via the third-party platform. Submitting information to the platform is assumed to take less time than submitting a SAR, as the type of information will be less detailed. The type of information is expected to be limited to customer identity information, such as name and address, and then a free text box where the reason for the information sharing can be entered.

51. It is estimated that submitting information about one customer to the third-party platform would take 30, 45 and 60 minutes (L, C and H). These are the estimates average times taken to submit a SAR, based on stakeholder survey responses.

52. For all firms, time has been valued using data from the Annual Survey of Hours and Earnings (ASHE) 2020, Table 14.5a. The analysis uses a median wage figure for administrative occupations: finance,

[26] Roughly 4,500 police officers have access to ELMER (data from UKFIU engagement for the SARs business case), and there are 137,582 police officers and 5,359 NCA staff as at 2021 Police workforce, England and Wales: 30 September 2021 - GOV.UK (www.gov.uk).

[27] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/936487/ESS_2019_Training_and_Workforce_Development_Report_Nov20.pdf. Figure in page 9, rounded up to £2,550.

Standard Occupational Classification (SOC) code 412, of £11.86 per hour[28], which is then uplifted by the non-wage share of costs of 22 per cent to reflect the marginal product of labour[29].

53. The number of submissions is assumed to be tied to SARs volumes which is assumed to increase at a constant rate of between 3 and 30 per cent each year, with a central estimate of 16 per cent per year (average based on the most recent five years of SARs data). The uncertainty around factors driving SARs volume growth trends informs the additional assumption that the growth rate applies for the second and third year in the modelled period before levelling off.

54. Table 5 represents the expected number of information submissions per year. This is based on taking the total SARs from financial firms each year[30] (which increase between 3 and 30 per cent for the second and third year before levelling off), multiplied by the proportion related to exiting a customer or refusing a service (a range of 10, 18 and 30 per cent, based on stakeholder survey responses), multiplied by the proportion of entities expected to submit information to the database (a range of 56, 58 and 60 per cent, based on stakeholder survey responses).

Table 5, Number of information submissions per year (000s), 2022/23 to 2031/32.

Year	Low	Central	High
2022/23	39	71	124
2023/24	40	82	160
2024/25	41	95	207
2025/26	41	95	207
2026/27	41	95	207
2027/28	41	95	207
2028/29	41	95	207
2029/30	41	95	207
2030/31	41	95	207
2031/32	41	95	207

Source: NCA SARs data 2016-2020, Home Office calculations, stakeholder survey, 2021.

55. The number of information submissions are then multiplied by the average time taken to submit to the platform (a range of 30, 45 and 60 minutes or 0.5, 0.75 and 1 hour, based on stakeholder survey responses), and the hourly FTE cost, which are presented in Table 6.

56. The values used to estimate the administration costs of information sharing are presented in Table 5 and 6 and are given as:

Number of information submissions (see Table 5) x average time to submit to the platform (see Table 6) x (median administrative occupations: finance wage x non-wage uplift of 22%)

Table 6, Administration costs for information submissions, £ million over 10 years, 2022.

Estimate	Average time to submit (hrs)	Cost per hour (£)	Total (£m PV)
Low	0.5	14.60	**2.4**
Central	0.75	14.60	**8.2**
High	1.0	14.60	**23.3**

Source: NCA, Assumption, ASHE 2020 Table 14.5a.

[28] Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics (ons.gov.uk) table 14.5a

[29] Non-wage cost is 17.9 per cent (from Eurostat), take 18/(100-18) = 18/82 = 22 per cent and uplift by this amount. https://ec.europa.eu/eurostat/databrowser/view/LC_LCI_LEV__custom_2052124/default/table?lang=en

[30] This includes the following sectors: Asset management, Banks, Building societies, Capital markets, Credit card, Electronic payment, Finance company, Mortgage provider, Other entities regulated by FCA, Specialist financial services, Stockbrokers

57. Total administration costs lie in a range of **£2.4** to **£23.3 million**, with a central estimate of **£8.2 million (PV over 10 years).** Given that the proposed measure is permissive, businesses are not obliged to act and set-up the IT platform, and as such this is classified as an indirect cost and not included in the BNPV or EANDCB.

Third party platform running costs to business

58. The specific approach to information sharing will not be prescribed by government, but it is assumed that firms will use a privately funded third party platform to facilitate information sharing. There will be ongoing running costs associated with hosting a third-party platform, which will be funded privately. Direct engagement with Cifas has informed that running costs for a similar platform would likely include employment costs[31], premises and office administration[32], company costs[33], member service costs[34] and communications costs[35] shown in Table 6. Employment costs are variable, whilst the other cost categories are fixed.

Table 7, Third party platform running costs per year, £ million, 2021/22.

Cost type	Cost element	Cost per year (£m)
Variable	Employment costs	5.4
Fixed	Premises and office administration cost	1.5
Fixed	Company cost	0.3
Fixed	Member service	1.7
Fixed	Communications	0.6

Source: Cifas

59. It has been assumed that only the variable elements of the platform running costs would increase as the number of SARs increases, as more SARs are expected to lead to more reports to the platform. However, there may be some economies of scale and therefore, it is assumed that running costs will increase at a slower rate than the overall increase in SARs. The low estimate assumes that there will be no increase in variable running costs, the central estimate assumes an increase of 3 per cent per year and the high estimate assumes an increase of 16 per cent per year in the second and third year before levelling off. This reflects the lag behind the range of the expected rise in SARs volumes.

Table 8, Total third-party platform running costs, £ million (PV) over 10 years, 2022).

Year	Low	Central	High
2022/23	4.8	4.8	4.8
2023/24	9.2	9.4	10.1
2024/25	8.9	9.2	10.7
2025/26	8.6	8.9	10.3
2026/27	8.3	8.6	10.0
2027/28	8.0	8.3	9.6
2028/29	7.8	8.1	9.3
2029/30	7.5	7.8	9.0

[31] Employment costs include salaries, national insurance, benefits and welfare, staff recruitment and development, travel and subsistence.

[32] Premises and office administration costs include Fixed office costs, Office maintenance and equipment, Office IT and telecommunications, Ancillary office costs, Depreciation.

[33] Company costs include Board costs, Corporate fees and subscriptions, Contingency.

[34] Member service costs include maintenance and development, Projects and research, Meetings, events and partnerships

[35] Communications costs include Public affairs, PR and marketing, Public telephone handling, Entertaining, Protecting the vulnerable.

2030/31	7.3	7.5	8.7
2031/32	7.0	7.3	8.4
Total	**77.5**	**79.9**	**90.7**

Source: Cifas, assumption, 2021.

60. In the first year of the appraisal period, running costs are assumed to be half of the annual running cost. This is due to an assumption that the database will take some time in the first year to be up and running to full utilisation.

61. These costs were provided in 2020/21 prices and have been inflated to 2021/22 prices for consistency. Total running costs for third party platforms lie in a range of **£77.5** to **£90.7 million (PV)**, with a central estimate of **£79.9 million (PV)** over 10 years**.** Given that the proposed measure is permissive, businesses are not obliged to act and set-up the IT platform, and as such this is classified as an indirect cost and not included in the BNPV or EANDCB.

Non-monetised costs

62. There may be some other administrative costs associated with data submission to the new utility, for example, additional staff familiarisation with the systems. Given that the information sharing measures are permissive, it is assumed that institutions who would incur large costs through participating would choose not to. Therefore, these costs are expected to be small and would represent a disproportionate effort to try and monetise as the data needed is not readily available.

Total costs

63. Total estimated costs lie in a range of **£87.1 to £160.3 million (PV)**, with a central estimate of **£105.5 million (PV)** over 10 years.

BENEFITS

Set-up benefits

64. There are no monetised set-up benefits for the proposed information sharing review.

Ongoing benefits

Crime displacement

65. Intelligence provided to LEAs through SARs reporting helps to prevent or disrupt criminals[36]. It is expected that, by sharing information where they have a suspicion of economic crime, businesses in the regulated sector will improve their internal intelligence and close down opportunities of criminal activities for criminals who have already been exited or refused a service by another regulated-institution, and in doing so, prevent crime. The main benefits estimated by this economic model are crimes prevented through closing down opportunities for criminals who have been refused service at one institution to simply conduct their criminal activity in a different institution.

66. Analysis commissioned by Home Office, conducted by Deloitte, has estimated the number of crimes that could be prevented by implementing private information sharing between regulated entities. The estimated number of crimes prevented is estimated using the:

- Expected number of eligible reports to the third-party database.
- Estimated usage of the third-party platform for both submitting and checking data.

[36] Evidence demonstrate the value of SARs intelligence in tackling a wide range of crimes. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file P.10.

- Conversion ratio from SARs reports to crime events prevented.
- Displacement.

67. The number of crimes prevented has been calculated by:

    a. Taking the total number of SARs from financial and credit institutions in 2020/2021 and uplifting them year on year by multiplying by a range of growth rates of 3, 16 and 30 per cent for the second and third year before levelling off. This gives the total number of SARs expected to be submitted by credit and financial institutions each year.

    b. Multiplying the total number of SARs per year by the proportion related to a customer exit or refusal of service. These proportions are a range of 10, 18 and 30 per cent (based on stakeholder survey responses these are the lowest, average and highest proportions). This gives the total number of reports eligible for sharing per year.

    c. To account for the fact that not all eligible reports will in fact be shared, a range of usage scenarios are applied, based on stakeholder survey responses. The range applied is 36, 37 and 38 per cent. The high estimate assumes that the platform would be free to use, the low estimate assumes use of the platform would require a subscription fee, and the best estimate takes the mid-point of these estimates. This gives the total number of actual reports to the platform.

    d. Multiplying by the conversion ratio from a report to a crime prevented. This is based on the assumption that not every report to the platform would have then led to a crime. This figure is 40 per cent, which is a proxy taken from direct engagement with Cifas, calculated by taking the number of reports to Cifas and dividing that by the number of crimes prevented as a result. To reflect uncertainty, 40 per cent has been taken as the high estimate, which has been halved and halved again to give the central and low estimate. This gives the estimated number of crimes disrupted.

    e. Multiplying the number of crimes disrupted by the percentage of displacement. It is not possible to close down all displacement opportunities. This is accounted for in the model through applying a range of displacement percentages. The percentage of displacement refers to how many crimes are simply displaced to elsewhere in the system, not actually prevented. For example, a displacement percentage of 90 per cent, means that 90 per cent of crimes are displaced and just 10 per cent are prevented. This analysis estimates the total crimes that are prevented, as opposed to simply displaced. A range of displacement percentages are applied, based on the dispersion of stakeholder survey responses. The range applied is 90, 70 and 50 per cent. This gives the total number of crimes prevented per year.

    f. The number of crimes prevented has then been multiplied by an estimated unit cost of crime to provide the estimated benefits of information sharing.

68. The unit costs of crime are a combination of published data and internal Home Office modelling[37]. The costs of crime are taken from the Home Office's Understanding Organised Crime (UOC) report 2016[38], the Home Office's Economic and Social Cost of Crime (ESCC) report 2018[39], the Experian Annual Fraud Indicator report 2017[40], the Department for Digital, Culture, Media and Sport (DCMS) Cyber Security Breaches Survey 2019[41], the Home Office Economic and Social Cost (ESC) of contact child sexual abuse report (CSA)[42] and Home Office internal analysis. The total number of financial crimes prevented does not only include direct prevention of fraud but also disruption of subsequent related offences, which could be drugs or other crimes. To reflect that not all crimes prevented would be fraud but could be other types of crime, a weighted average cost of crime has

[37] 10 of the unit costs are from published data, and only drug offences have been modelled by the Home Office.

[38] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782656/understanding-organised-crime-mar16-horr103-2nd.pdf

[39] The economic and social costs of crime second edition - GOV.UK (www.gov.uk)

[40] annual-fraud-indicator-report-2017.pdf (experian.co.uk)

[41] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

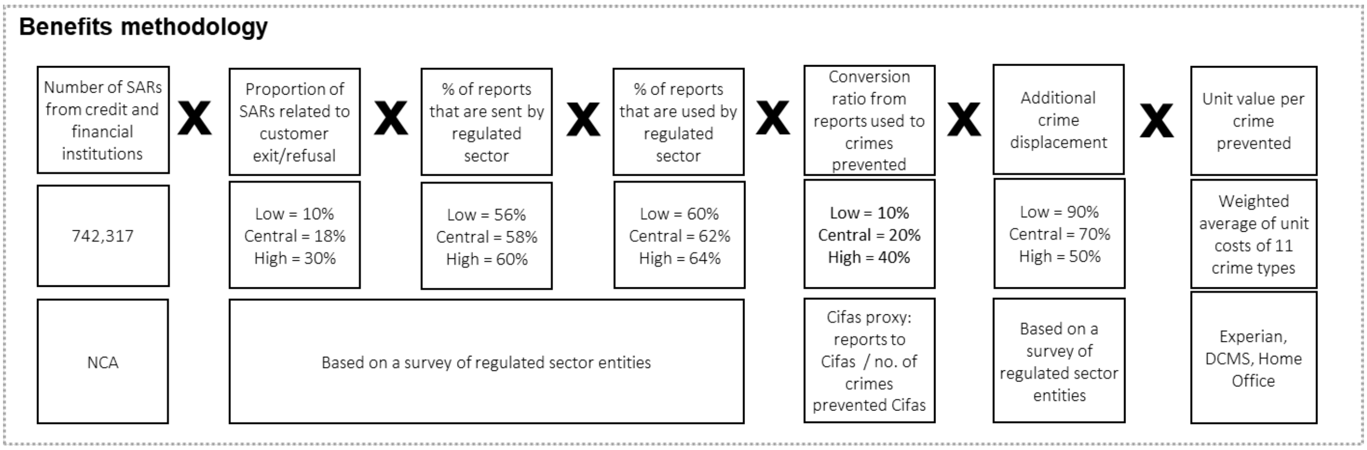
[42] The economic and social cost of contact child sexual abuse - GOV.UK (www.gov.uk)

been calculated. The weighted average unit cost of crime across fraud, drug and other crime (comprising 9 threat types[43]) has been calculated by taking the unit cost of a fraud crime and the estimated cost of drug and other crimes prevented through disruption. Then, the mean of these costs is taken to get a weighted average unit cost.

69. Figure 1 shows the benefits methodology.

[43] Child sexual abuse (CSA), Organised Immigration Crime (OIC), Modern Slavery and Human Trafficking, Money Luandering, Bribery, International Corruption and Sanctions Evasion, Cyber Crime, Firearms, Organised Acquisitive Crime (OAC), Border Vulnerabilities.

Figure 1, Benefits methodology for estimate of crime displacement, 2022.



Benefits methodology

Number of SARs from credit and financial institutions	X	Proportion of SARs related to customer exit/refusal	X	% of reports that are sent by regulated sector	X	% of reports that are used by regulated sector	X	Conversion ratio from reports used to crimes prevented	X	Additional crime displacement	X	Unit value per crime prevented
742,317		Low = 10% Central = 18% High = 30%		Low = 56% Central = 58% High = 60%		Low = 60% Central = 62% High = 64%		**Low = 10%** **Central = 20%** **High = 40%**		Low = 90% Central = 70% High = 50%		Weighted average of unit costs of 11 crime types
NCA		Based on a survey of regulated sector entities						Cifas proxy: reports to Cifas / no. of crimes prevented Cifas		Based on a survey of regulated sector entities		Experian, DCMS, Home Office

Source: Internal Home Office modelling, 2022.

70. Table 9 shows the number of crimes prevented each year under **Option 2**, which are then multiplied by the weighted average unit cost of crime to estimate the total benefits. Total benefits from prevented crimes is estimated in a range of **£17.4 million** to **£1.70 billion**, with a central estimate of **£238.1 million (PV over 10 years).**

Table 9, Estimated volume of crimes prevented, 2022/23 to 2031/32.

Year	Low	Central	High
2022/23	200	3,000	16,000
2023/24	300	3,000	21,000
2024/25	300	4,000	27,000
2025/26	300	4,000	27,000
2026/27	300	4,000	27,000
2027/28	300	4,000	27,000
2028/29	300	4,000	27,000
2029/30	300	4,000	27,000
2030/31	300	4,000	27,000
2031/32	300	4,000	27,000

Source: Stakeholder workshops, NCA, Cifas, Home Office internal analysis, UOC 2016[44], ESCC 2018[45], Experian Annual Fraud Indicator report 2017[46] , DCMS 2019[47], ESC CSA report 2021[48].

71. Credit and financial institutions will also be able to submit information about a customer they have suspicions about *before* they have submitted a SAR, or taken action against the customer, but it has not been possible to estimate the number of eligible reports.

72. Credit and financial institutions currently submit a significant amount of SARs (approximately 742,317 in 2020/2021)[49], and not all of these SARs lead to action being taken against a customer. This suggests that credit and financial institutions already act with a significant level of caution when they have concerns about potential financial crime, and this was reflected in the stakeholder consultation. It is assumed that in the majority of cases where credit and financial institutions have any suspicion of financial crime, a SAR will be submitted.

[44] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782656/understanding-organised-crime-mar16-horr103-2nd.pdf
[45] The economic and social costs of crime second edition - GOV.UK (www.gov.uk)
[46] annual-fraud-indicator-report-2017.pdf (experian.co.uk)
[47] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019
[48] www.gov.uk/government/publications/the-economic-and-social-cost-of-contact-child-sexual-abuse
[49] https://nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020

73. It is possible that the benefits would be greater as firms can share information under a broader range of scenarios than the one modelled, but this has not been possible to monetise.

Cost savings to business

74. Currently, as well as missing opportunities to prevent crime upstream, regulated entities incur unnecessary remediation and onboarding costs, including investigating and exiting customers (where there can be a 60-day notice period). Increased information sharing is expected to improve the efficiency of customer onboarding, due diligence and remediation. Information sharing would presumably lead to regulated entities taking on fewer criminals as they know they have been 'debanked' by another bank, saving time and money.

75. The onboarding and due diligence estimates presented earlier (paragraphs 11a and b) are not considered as estimates of the potential benefits to business because of the high degree of uncertainty. Instead, due to the permissive nature of the proposed measure, it is expected that businesses will act if the benefit of acting is at least as large as the cost of implementing the IT platform, which informs the assumptions about benefits. For the central scenario, it is assumed that the benefit to business equals the central estimate of the set-up and running costs of the IT platform[50]. The low and high estimates are set at 75 and 125 percent of the central estimate of the IT platform's setup and running costs, respectively.

Table 10, Cost savings to regulated sector, £ million (PV) over 10 years, 2022).

Year	Low	Central	High
2022/23	16.9	22.5	28.1
2023/24	7.7	10.3	12.8
2024/25	7.7	10.2	12.8
2025/26	7.4	9.9	12.3
2026/27	7.2	9.5	11.9
2027/28	6.9	9.2	11.5
2028/29	6.7	8.9	11.1
2029/30	6.5	8.6	10.8
2030/31	6.2	8.3	10.4
2031/32	6.0	8.0	10.0
Total	**79.1**	**105.4**	**131.8**

Source: Home Office Estimates, 2021.

76. Total estimated benefits to businesses lie in a range of **£79.1 million to £131.8 million**, with a central estimate of **£105.4 million (PV)** over 10 years. Despite the fact that the proposed measures have a direct impact on the ability of the regulated sector to share information, they do not have a direct impact on the cost of onboarding and due diligence. Onboarding and due diligent costs could be impacted by second order effects where businesses, upon having access to better intelligence, may decide against onboarding risky customers, eliminating associated costs. Since these impacts are second order, they are not included as direct benefits in the BNPV or EANDCB.

Non-monetised benefits to business

77. Trust and confidence in the regulated sector could be increased if there is a reduction in money laundering facilitated as a result of these policies.

[50] The costs include set-up, training, administration costs and running of IT platform.

78. Cifas is an existing information sharing platform for fraud and sharing in this platform is estimated to have **prevented £1.4 billion of fraud in 2020**[51], although fraud is more widespread than the other forms of economic crime (that is, money laundering and corruption). It is possible that the broader information sharing measures proposed might also indirectly help detection and prevention of fraud, but this has not been modelled due to significant uncertainty.

Total benefits

79. Total estimated benefits lie in a range of **£96.4 million to £1.84 billion**, with a central estimate of **£343.6 million (PV)** over 10 years.

Total costs and benefits, NPSV, BNPV and net direct cost to business

80. The estimate of total cost for **Option 2** lies in the range **£87.1 to £160.3 million (PV)** with a central estimate of **£160.3 million (PV)** over 10 years. The total monetised benefits lie in the range **£96.4 million to £1.84 billion**, with a central estimate of **£343.6 million (PV)** over 10 years.

81. The Net Present Social Value (NPSV), which is the total discounted benefits minus the total discounted costs, lies in a range of **£9.4 million to £1.675 billion**, with a central estimate of **£238.0 million** over the 10-year appraisal period.

82. The Business Net Present Value (BNPV) is estimated to lie in the range **£0.0 to £0.0 million** with a central estimate of **£0.0 million** over 10 years.

83. The net direct cost to business (EANDCB[52]) is estimated to lie in the range **£0.0 to £0.0 million (PV)** with a central estimate of **£0.0 million (PV)** over 10 years.

Direct costs to business

84. Table 11 displays the NPSV, the BNPV, and the net direct cost to business. Estimates are in 2021/22 prices with a present value base year (PVBY) of 2022/23.

Table 11, Summary of costs, benefits, NPSV, BNPV and EANDCB over 10 years (£m PV), 2022.

Costs	**Low**	**Central**	**High**
Total set up costs	7.2	17.4	46.4
Total ongoing costs	79.9	88.1	114.0
Total costs	**87.1**	**105.5**	**160.3**
Total benefits	**96.4**	**343.6**	**1,835.5**
NPSV	9.4	**238.1**	1,675.2
BNPV	0.0	0.0	0.0
EANDCB	0.0	0.0	0.0

Source: Home Office internal analysis, 2022.

[51] Fraudscape 2021 - Cifas

[52] The net direct cost to business is defined as the Equivalent Annual Net Direct Cost to Business.

Value for money (VfM)

85. For a policy to be considered VfM, it must achieve the strategic and policy objectives. **Option 2** is likely to meet the policy objectives of enabling information sharing between regulated entities where there is suspicion of economic crime, as it will allow firms to engage in private-to-private information sharing. It is likely to meet the strategic objective of reducing crime, as increasing information sharing between credit and financial firms will improve their intelligence picture, allowing them to avoid onboarding criminals who have already been refused a service elsewhere due to suspicion of economic crime and helping businesses to spot criminal networks across different providers. This will disrupt criminal activity and help to prevent the displacement of crime, where criminals who are exited or refused a service from one institution are able to exploit the system through other service providers.

86. Overall, the proposed measure is expected to address inefficiency, reduce costs, and potentially result in a more efficient allocation of resources. The measures – if implemented – could result in benefits of **£343.6 million** over 10 years. Although the majority of the estimated costs are borne by businesses, as explained, they will only act if the benefits outweigh the costs for them, and as such, these are classed as indirect costs. The estimated potential costs of onboarding problem customers compared to the IT platform costs points to an efficiency gain for businesses (see paragraph 11). The NPSV of **£238.1 million** indicates the benefits outweigh the costs of this policy, with the crime reduction expected to have positive effect on the social welfare of UK residents. The benefits modelled may be under-estimate, because they do not model the whole range of scenarios under which information can be shared and it is possible that more crimes can be prevented than the numbers modelled.

Impact on small and micro-businesses

87. According to Business Population Estimates 2021, around 99 per cent of the total business population is made up of small businesses (0 to 49 employees) [53]. Small and micro-businesses make up the majority of the financial and credit sector by number of businesses. These measures are legislative exemptions which are not targeted at small and micro-businesses but will affect them as members of the regulated sector. The preferred option is a permissive measure and so there is a reasonable expectation that business will adopt these changes only where they lead to net benefits for business. This should ensure that there are no disproportionate burdens on small and micro-businesses. The proposed options are all estimated to have a benefit for businesses as they are designed to improve the ability for businesses in the regulated sector to assess risk. If SMBs decide not to participate in information sharing, the IT platform cost is avoided, however, the potential benefit of avoiding the onboarding risky customer is not realised by SMBs. It is not expected that larger firm gain a disproportionate advantage over SMBs as a result of this, but it means SMBs wouldn't have this addition information to tackle risky customers

F. Proportionality

88. As this is a Final Stage IA, efforts have been made to monetise impacts as far as possible, making use of from findings from the Home Office targeted consultations with the regulated sector and LEAs. The impact estimates associated with the proposed changes are indicative only.

89. Whilst this IA would have benefited from the monetisation of all the identified benefits and costs, a proportional approach was taken to monetise benefits and costs that were considered to have material impacts, with those expected to have minimal impacts unmonetised. In most cases of unmonetised benefits or costs, there was either a lack of data or considerable data challenges. The analysis has considered all relevant costs to businesses.

[53] 2021 Business population estimates for the UK and the Regions: Statistical Release (publishing.service.gov.uk)

G. Risks

Financial inclusion

90. The proposal involves sharing personal data about customers in order to help inform other businesses risk-based decisions about taking on or retaining these customers. While the aim is to prevent bad actors exploiting the financial system, there is a risk that information on the system about a customer could lead to individuals being excluded from a wider range of products and services than they already are. While the number of customers denied products or services is unlikely to increase from present levels, these customers are likely to find an increased number of businesses denying them products or services. An Equalities Impact Assessment has found that the proposal is not likely to disproportionately impact any group with a protected characteristic.

91. Although the measures should only impact those who have been involved in criminal activity, individuals being more broadly excluded from products or services could lead to increased risk of economic harm. For example, individuals who have been excluded due to suspicions of criminal activity may not be able to access banking services even for legitimate purposes, which could cause them economic harm.

92. The Government is clear that businesses involved in sharing customer information must have adequate safeguards in place to guard against the risk of unsubstantiated financial exclusion, and that innocent individuals who have suffered exclusion as a result of having their information shared can access effective avenues for redress. This will also protect businesses involved in sharing customer information against the risk of suffering reputational damage or being required to pay fines/compensation if customers are not properly safeguarded. The economic risk to businesses could be substantial, as if a firm were to misuse customer data it would be liable for a data breach under UK UK GDPR and maybe subject to an infringement fine. The UK UK GDPR 2018 and DPA 2018 set a maximum fine of £17.5 million or 4 per cent of annual global turnover – whichever is greater – for infringements. It is the Government's view that the existing mechanisms that enable individuals to appeal against financial exclusion provide the right framework for any future appeals based on private to private information sharing, without the need for further legislation.

93. A businesses existing obligation around data accuracy, integrity, purpose, storage and accountability under UK GDPR 2018 will continue to apply. Article 5(1) of UK GDPR 2018 requires that information shared should be:

    a. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').

    b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation').

    c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

    d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

    e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation').

    f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

94. Additionally, the PAR 2015 provide the right to a basic bank account even for customers who have been excluded products by other providers. The Regulations make it clear that such a basic account can only be terminated in specific circumstances such as knowingly using the account for illegal purposes, but not because of unlawful bias or discrimination and can only be refused in specific circumstances including that doing to would be contrary to the MLRs. Non-compliance with the Regulations can lead to penalties from the FCA including financial penalties.

95. Finally, financial firms are required by the FCA to treat customers fairly. See: FCA Principles for Customers and PRIN for Firms[54]. The FCA's Principles for Business include explicit and implicit guidance on the fair treatment of customers. Principle 6 says: '*A firm must pay due regard to the interests of its customers and treat them fairly*', but other principles also apply to this area of business behaviour. In February 2021, the FCA published finalised Guidance[55] setting out their view of what firms should do to comply with their obligations under the Principles and take particular care to ensure vulnerable customers are treated fairly.

96. It is believed that these existing obligations under UK GDPR 2018, the right to a Basic Bank Account, and FCA guidance provide the necessary protections for customers

Analytical risk

97. The estimated benefits rely on businesses implementing a new IT platform. The value for money assessment is dependent on business acting, taking advantage of the new legislation, and implementing a new IT platform. It is not certain businesses will act on the new legislation, but evidence suggests they have an incentive to do so because data suggests approximately 761,500 customers were exited[56] from all lines of business for financial crime reasons[57]. Some of the costs of onboarding and performing due diligent on these customers could be avoided if information from any new IT platform can screen out some of these customers. So, although there is a risk that the estimated benefit through reduction in crime might not be realised, this risk is low because businesses have a strategic rationale to act.

98. The SARs volumes have been rising year-on-year and a growth rate based on past data has been used to model the central scenario in this analysis. However, growth in SARs volumes has been volatile so there is a risk that the number of SARs submitted each year rises at a lower, or higher rate than the range modelled here. A higher volume of SARs may increase the administration burden of information sharing for businesses. However, this would also be expected to increase the potential benefits, so the impact of an increased volume of SARs on the net benefits is expected to be positive.

99. Many of the cost/benefit estimations rely on data from a stakeholder workshop with the regulated sector facilitated by Deloitte. The workshop had participants from 14 different firms from the regulated sector. These firms came from a variety of different regulated subsectors. This was the best data available but there is a risk of relying on responses from a small sample size, as that sample may not be representative of the whole credit and financial sector. Nevertheless, one respondent to the survey was responsible for roughly one third of the total SARs submitted to the NCA in 2020. And as such, there is a considerable degree of confidence that the data provided is representative of the credit and financial sector.

100. The benefits analysis relies on the assumption that firms will submit information to a platform once their suspicion has already led to them taking action against a customer (for example, refusing a service or exiting the customer), as the data received from the stakeholder survey is based on this scenario. However, the legislation will allow businesses to submit information under a broader range

[54] FCA Principles for Customers and PRIN for Firms | FCA

[55] Guidance for firms on the fair treatment of vulnerable customers | FCA

[56] According to the FCA:"This covers any customers or clients with whom the firm ceased to do business where financial crime or criminal behaviour by a customer or client with a financial element was the principle driver behind the decision."

[57] Financial Crime: analysis of firms' 2017-2020 REP-CRIM data | FCA

of scenarios, which have not been modelled due to significant uncertainty around expected usage and the expected benefit of sharing intelligence about a customer where the bank has not yet considered them sufficiently suspicious to take any action. It is possible that businesses would use the platform under a broader range of scenarios than modelled and that this could change the overall net benefit. However, increased information sharing under a broader range of scenarios is expected to lead to more opportunities to disrupt crime, which would have a positive impact on the net benefit. This risk that the data is misused is expected to be mitigated via Article 5(1) of UK GDPR 2018.

H. Wider impacts

101. There are no anticipated wider impacts of these proposals.

I. Trade Impact.

102. There are no anticipated trade or investment implications of the measure.

J. Monitoring and evaluation (PIR if necessary)

103. The proposal is at final stage. There are no new monitoring and evaluation plans as the proposed legislative measures are amendments that current systems can monitor.

104. An indicator that will be monitored is banks deciding to set up a third party platform and engage in information sharing, as this would suggest that banks see that the benefit to participation in information sharing outweighs the costs. In addition, the number of entities signed up to use the platform will be monitored.

105. The number of customers debanked (exited) from deposit-taking bodies and payment institutions due to suspicion of money laundering would be monitored. If these measures result in more criminals being denied banking services it would suggest that information sharing is having the desired effect of improving banks’ ability to assess risk. It is assumed that entities already collect this data internally and engagement with banks would be required to obtain this data.

106. Offences are currently recorded centrally in Home Office data and this system will not change. Any reduction in crime rates as a result of information sharing measures will be tracked by the current system.

107. A post-implementation review will be undertaken in October 2026, about three years after Royal Assent to allow the policy to embed and for routine monitoring and feedback from stakeholders to be used ensure any initial issues are dealt with.

Impact Assessment Checklist

Mandatory specific impact test - Statutory Equalities Duties	Complete
Statutory Equalities Duties An Equalities Impact Assessment has found that the proposal is not likely to disproportionately impact any group with a protected characteristic. The proposal involves sharing personal data about customers in order to help inform other businesses risk-based decisions about taking on or retaining these customers. While the aim is to prevent bad actors exploiting the financial system, there is a risk that information on the system about a customer could lead to individuals being excluded from a wider range of products and services than they already are. While the number of customers denied products or services is unlikely to increase from present levels, these customers are likely to find an increased number of businesses denying them products or services. The Government is clear that businesses involved in sharing customer information must have adequate safeguards in place to guard against the risk of unsubstantiated financial exclusion, and that innocent individuals who have suffered exclusion as a result of having their information shared can access effective avenues for redress. It is the Government's view that the existing mechanisms that enable individuals to appeal against financial exclusion provide the right framework for any future appeals based on private-to-private information sharing, without the need for further legislation. A business' existing obligations around data accuracy, integrity, purpose, storage and accountability under UK GDPR will continue to apply. Article 5(1) of UK GDPR is explained in paragraph 90 a-f. **The SRO has agereed these summary findings from the Equality Impact Assessment.**	**Yes**

Any test not applied can be deleted except **the Equality Statement**, where the policy lead must provide a paragraph of summary information on this.

The Home Office requires the **Specific Impact Test on the Equality Statement** to have a summary paragraph, stating the main points. **You cannot delete this and it MUST be completed**.

Economic Impact Tests

Business Impact Target The Small Business, Enterprise and Employment Act 2015 (s. 21-23) creates a requirement to assess the economic impacts of qualifying regulatory provisions on the activities of business and civil society organisations. [Better Regulation Framework Manual] The BIT Score is the direct cost to business over the whole reporting period. This is equal to the EANDCB x 5 (the term of the Parliament). The BIT score for the information sharing legislation has been calculated as **£0.0 million**, this is due to the both the potential costs and benefits to business being deemed as indirect.	**Yes**

Small and Micro-business Assessment (SaMBA) The SaMBA is a Better Regulation requirement intended to ensure that all new regulatory proposals are designed and implemented so as to mitigate disproportionate burdens. The SaMBA must be applied to all domestic measures that regulate business and civil society organisations, unless they qualify for the fast track. [Better Regulation Framework Manual] These measures are legislative exemptions which are not targeted at small and micro-businesses but will affect them as members of the regulated sector. The preferred option is a permissive measure and so there is a reasonable expectation that business will adopt these changes only where they lead to net benefits for business. This should ensure that there are no disproportionate burdens on small and micro-businesses. The proposed options are all estimated to have a benefit for businesses as they are designed to improve the ability for businesses in the regulated sector to assess risk.	**Yes**