

Title: Criminal Finances Act – Information Sharing IA No: HO0289 RPC Reference No: RPC-3494(1)-HO Lead department or agency: Home Office Other departments or agencies: National Crime Agency	Impact Assessment (IA)			
	Date: 20-06-2017			
	Stage: Enactment			
	Source of intervention: Domestic			
	Type of measure: Primary legislation			
Contact for enquiries: public.enquiries@homeoffice.gsi.gov.uk				
Summary: Intervention and Options				RPC Opinion: GREEN

Cost of Preferred (or more likely) Option				
Total Net Present Value	Business Net Present Value	Net cost to business per year (EANDCB in 2014 prices)	One-In, Three-Out	Business Impact Target Status
£m	£m	£m	Not in scope	Qualifying provision

What is the problem under consideration? Why is government intervention necessary?
 In October 2015, the Government published the National Risk Assessment for Money Laundering and Terrorist Financing (NRA), identifying a number of areas where the response to these threats could be strengthened. Both the private sector and the law enforcement agencies hold significant amounts of data on individuals and legal entities. The nature of money laundering is that illicit funds move across the reporting sector and through business structures, and only the private sector entities can see how those flows or interactions occur. Previously, there was limited legal cover from civil liability for private sector entities to share data that falls under the Data Protection Act, so we have introduced a legal provision to provide such a mechanism.

- What are the policy objectives and the intended effects?**
- Facilitate information sharing between regulated sector entities for intelligence gathering in relation to a suspicion of money laundering.
 - Enable firms better to protect themselves from money laundering and terrorist financing risks.
 - Enable the production of better quality suspicious activity reports from the private sector.
 - More informed investigations by law enforcement agencies, leading to better anti-money laundering outcomes.

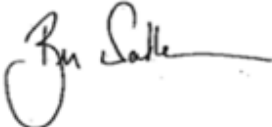
What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

1. Do Nothing
 There is already cover from breaching the Data Protection Act where data sharing is for the purpose of preventing or detecting crime. However, this does not provide civil liability cover for those sharing data, and leaves firms open to action in the civil courts by their customers.

2. Provision of a model to support voluntary data sharing
 We will deliver provisions that allow the private sector to share data in order to prevent and detect crime without legal risk.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: By 03/2022				
Does implementation go beyond minimum EU requirements?			N/A	
Are any of these organisations in scope?			Micro Yes	Small Yes
			Medium Yes	Large Yes
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)			Traded:	
			Non-traded:	

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  Date: 20-06-2017

Summary: Analysis & Evidence

Policy Option 1

Description: Do nothing

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low: Optional	High: Optional	Best Estimate:

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional	Optional	Optional
High	Optional	Optional	Optional
Best Estimate			

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

There are no monetised costs.

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

There would continue to be no legal mechanism for private sector entities to share detail on suspicious activity with confidence. As a result opportunities to share information, protect themselves from money laundering risk, and develop better quality suspicious activity reports will be missed.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional	Optional	Optional
High	Optional	Optional	Optional
Best Estimate			

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

None

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

None

Key assumptions/sensitivities/risks (%)	Discount rate	
---	---------------	--

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs:	Benefits:	Net:	

Summary: Analysis & Evidence

Policy Option 2

Description: Legislate to support information sharing

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low: Optional	High: Optional	Best Estimate:

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional	Optional	Optional
High	Optional	Optional	Optional
Best Estimate			

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

There are no monetised costs.

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

There will be gross costs incurred by the regulated private sector for sharing data between themselves and with law enforcement. There will also be minimal familiarisation costs. However since this is a voluntary measure, it is assumed the benefits to the private sector would outweigh the costs.

Law enforcement could face opportunity costs from investigations begun as a result of better intelligence.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional	Optional	Optional
High	Optional	Optional	Optional
Best Estimate			

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

None

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

Encourage greater data and information sharing from the reporting sector, leading to more insightful suspicious activity reports (SARs) available to law enforcement.

Allow the private sector to take measures to better protect themselves from money laundering.

Investigations provided with better information, leading to improved anti money laundering and terrorist finance outcomes.

Key assumptions/sensitivities/risks (%)

Discount rate

Regulated sector private entities will share data for the purposes of developing better SARs as it will be beneficial to them, as suggested in consultation.

Potential cost to privacy, mitigated by expected standards and continued private sector compliance with the Data Protection Act.

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs:	Benefits:	Net:	

Evidence Base (for summary sheets)

A. Strategic Overview

A.1 Background

1. Financial profit is the driver for almost all serious and organised crime, and other lower-level acquisitive crime. The UK drugs trade is estimated to generate revenues of nearly £4bn each year and HMRC estimate that over £5bn was lost to attacks against the tax system in 2012/13. Criminals launder their money – moving, using and hiding the proceeds of crime – to fund their lifestyles and to reinvest in their criminal enterprises. The best available estimate¹ of the amounts laundered globally are equivalent to 2.7% of global GDP, or US\$1.6 trillion in 2009, while the National Crime Agency assesses that billions of pounds of proceeds of international corruption are laundered into or through the UK. This threatens the integrity and reputation of our financial markets.
2. In October 2015, the Government published the National Risk Assessment for Money Laundering and Terrorist Financing (NRA), identifying a number of risks and areas where the regimes that combat those threats could be strengthened. The Action Plan for anti-money laundering and counter-terrorist finance, published in April 2016, contained a range of measures to build on the UK's risk-based approach to addressing these areas. The Criminal Finances Act is a core part of our approach to achieving that objective.
3. The current legal framework for data protection allows firms to share data with one another on those they suspect of being involved in money laundering, but at the risk of facing civil action for doing so. The Proceeds of Crime Act 2002 (POCA) provides legal cover for firms to make disclosures about suspicions of money laundering to the National Crime Agency (NCA) (by submitting a suspicious SAR).
4. The Joint Money Laundering Intelligence Taskforce (JMLIT) was founded in 2015 in order to enable financial sector institutions and law enforcement agencies to share and analyse information to prevent, detect and disrupt money laundering. JMLIT participants use the data sharing gateway available to the NCA under s7 of the Crime and Courts Act. However, this would not work for data sharing where the NCA is not involved, and financial sector participants have sought a new information sharing gateway that will enable direct firm-to-firm information sharing under legal 'safe harbour' (i.e. with protection from criminal or civil liability when information has been shared in good faith).
5. Banks are subject to both general UK data protection legislation, and to banking-specific legislation and case law. Client confidentiality case law places restrictions on what banks can do in relation to sharing customer data. *Tournier v National Provincial and Union Bank of England, Ltd [1923]* established implied contractual terms that bank customer information is confidential, but that a bank may disclose confidential customer information:-
 - where disclosure is required by law (for example, under a court order);
 - where there is a duty to the public to disclose (for example to prevent frauds or crimes);
 - where the legitimate interests of the bank require disclosure (for example to recover a debt); or,
 - where the disclosure is made by the express or implied consent of the customer.
6. The "duty to the public" provision of *Tournier* pre-dates data protection legislation, and the burden of proof is placed on the private sector to prove public interest. This has led to banks seeking primary legislation to remove the legal risks they face. Banks can manage customer confidentiality through their terms and conditions of business (i.e. by replacing the implied contractual terms of *Tournier* with explicit contractual terms) but relying on this approach would not provide a single consistent legal standard to encourage voluntary sharing.

¹ *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, UNODC 2011

7. General data protection law does not preclude the sharing of personal account data between private sector entities, provided that the requirements in the Data Protection 1998 (DPA) and the EU General Data Protection Regulation (GDPR), respectively, are met. The GDPR is not yet in force, as there is an implementation period of two years ending on 25 May 2018. Banks currently comply with the various EU member state laws implementing the EU Data Protection Directive (95/46/EC) – such as the UK DPA. However, in doing so, they are potentially liable for claims for damages from individual customers for breach as well as fines or criminal enforcement by the relevant data protection regulator (such as the UK Information Commissioner). Note that notwithstanding the UK's vote to leave the EU, it is widely expected that the GDPR – or national terms of equivalence – will apply to UK banks whether or not the UK is in the process of leaving the EU on 25 May 2018 and/or leaves thereafter.
8. The DPA overlaps with the issue of confidentiality, by implementing a series of rules called the "non-disclosure provisions". These are statutory confidentiality rules. The non-disclosure provisions do not apply where a disclosure is "necessary for the prevention and detection of crime". The banks are generally anxious about relying upon the exemption from the non-disclosure provisions when sharing information with each other as the burden is upon them to prove that the disclosure is "necessary for the prevention and detection of crime" on the basis that other banks don't have a statutory or other function relating to the "prevention and detection of crime" which would provide a more explicit gateway.
9. Personal information about the suspicion of money laundering is "sensitive personal data" under the DPA – being information relating to criminal or alleged criminal offences. As such the banks need to fall within a DPA Schedule 3 processing condition to share the personal information. This is easy when sharing with a law enforcement agency, as the conditions include "the administration of justice" and "Crown" functions. The only Schedule 3 processing conditions the banks can rely upon to share information with each other is "substantial public interest". However, this is a relatively high threshold to prove, particularly where other banks don't have a statutory or other function relating to the "prevention and detection of crime" (notwithstanding their legal and regulatory obligations to identify and minimise money laundering).
10. Under the GDPR, "processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards". It is likely that JMLIT/AML activity undertaken by banks will constitute "related security measures" and as such these criteria will need to be met, including the requirement that the activity be authorised by law.

A.2 Groups Affected

11. The groups affected by this legislation include:
 - Law enforcement agencies, including the NCA, National Policing, HM Revenue and Customs, the Serious Fraud Office, and other prosecuting authorities.
 - Entities in the regulated sectors i.e. banks, accountancy firms, lawyers, estate agents.
 - Regulatory bodies, such as the Financial Conduct Authority.
 - The general public, whose safety and security is impacted by the threat of serious and organised criminals.

A.3 Consultation

Within Government

12. Prior to the Bill's introduction, we consulted HM Treasury, law enforcement agencies, and with counter terrorist financing colleagues.

Public Consultation

13. The public consultation took place through the Action Plan for anti-money laundering and counter-terrorist finance, which was published on 21 April 2016, with the consultation finishing on 2 June 2016.
14. We further consulted on data sharing with the private sector, particularly the banks, to obtain their views on our proposals.
15. Following the introduction of the Bill, consultation with law enforcement agencies and the private sector was maintained to ensure that they could continue to provide their views and help shape this measure during the Bill's passage. For example, the timeframe for the voluntary sharing of information was increased from 28 days to 84 days following advice from the regulated sector that 28 days might not be long enough for effective information sharing.

B. Rationale

16. Both the private sector and the law enforcement agencies hold significant amounts of data on individuals and legal entities. The private sector holds data on financial transactions and related personal data; the law enforcement agencies hold details of criminals, and intelligence on crime. When this data has been shared, such as under JMLIT, there have been benefits to both sectors. But the level of sharing was limited by concerns about the legal framework under which information is shared. The nature of money laundering is that illicit funds move across the reporting sector and through business structures, and it may be that only the private sector entities can see how those flows, or the interactions between money launderers, occur. Having the ability for a group of firms to share information directly with one another, either at their own instigation, or on request from the NCA, would have significant benefits.
17. Reporting sector institutions have asked that we consider providing legal cover to allow them to implement data sharing between individual institutions for the purpose of developing more detailed and accurate SARs, and to help them to protect themselves more effectively from the risks of money laundering. Where individual institutions identify individuals or accounts they suspect of being involved in money laundering or terrorist financing, they wish to be able to share their own data, or to request it from others. Law enforcement agencies are supportive of this approach.

C. Objectives

18. The policy aims are to encourage greater data and information sharing from the reporting sector, better to harness the private sector's understanding of the flows of transactions and entities engaged in money laundering, terrorist financing or other criminal activity.
19. This will lead to better quality SARs submitted by the reporting sector, more effective insight drawn from information across private sector entities, and therefore higher quality intelligence available to law enforcement agencies.
20. Law enforcement will have better insight to fight financial crime, including money laundering and terrorist finance.
21. Firms will be able better to protect themselves as they develop a fuller understanding of the money laundering risks they face.

D. Options

22. The following options have been considered:

- Option 1 was to make no changes (do nothing).
The private sector has indicated that without such legislative cover they would be unwilling to share data between themselves.
- Option 2 (Preferred) was to amend POCA and mirror these changes in the Terrorism Act 2000 to support data sharing between the NCA and the private sector, and between private sector entities.

FURTHER DETAIL ON OPTION 2

Data sharing request between firms at the request of the NCA

23. The NCA, through its own intelligence work, or through the analysis of SARs, may identify that there would be a benefit for a regulated sector entity to share information voluntarily with another. The information may relate to a person, a legal person, or to wider information such as transactions between particular entities.
24. The NCA is able to request an entity to share information voluntarily with another and provide a collective report. The NCA has to state why and what information is required.
25. In supporting the NCA request the entities have been provided with defined legal cover that removes the risk of civil liability for sharing that data, unless the sharing was done negligently or maliciously. It will be for each entity to determine whether they wished to contribute information, and there is no penalty if they decline.
26. The NCA already had the power to share information through the provisions in Section 7 of the Crime and Courts Act 2013 (CCA). It did not, however, have an express statutory power to request information to be shared voluntarily or to provide the respondent with cover from civil liability for sharing such information other regulated sector entities, although it had residual powers to request information from any person or entity.
27. We believe that there should be an explicit provision that permits the NCA to request information on money laundering and terrorist financing to be shared by one entity on a voluntary basis with another. The provision sets the terms for the use of the request, including specifying:
 - a. The reason for the request, and the basis for it being made;
 - b. The subject of the request, and the type of information being looked for;
 - c. The date by which a response is needed.
28. This provision is not intended to be a substitute for gathering evidence for a case. Those powers already exist in Part 8 of POCA, and is intended to allow the NCA to gather more information / intelligence.

Data sharing between regulated sector entities initiated by a firm

29. Regulated sector entities may wish to share data between themselves for the purpose of identifying or confirming suspicious activity. The participants in the JMLIT have reported to Government that they need a new legal gateway to encourage greater and quicker information sharing. Banks have also asked for legal cover to allow them to collaborate to provide better and more detailed SARs. The regulated sector is already able to do this to some extent through the DPA sch29, but that does not provide cover from civil litigation.
30. The regulated sector wanted to be able to seek data from, and share data between a range of entities, including:
 - To a separate legal entity (e.g. bank to bank);
 - With a subsidiary company;
 - With a subsidiary in another country, provided that this did not conflict with existing data protection requirements in another country.

31. The key concern for the regulated sector was that they are provided with a defence against civil action for sharing personal data, unless the sharing is malicious or negligent. This is already done for SARs, although the provision of these is a legal requirement on the regulated sector.
32. We have introduced a provision to support the regulated sector in sharing data between themselves, but in providing a significant level of cover from civil litigation, this must be used only where there is a suspicion of money laundering. Any output where suspicion of money laundering exists must be shared with the NCA.
33. The data sharing should be the responsibility of the nominated officer for each entity. Any data sharing between firms should be recorded, in order for the safe harbour provisions to apply. The record would need to be available for audit by the appropriate regulator, or at the order of a court. The regulated sector should be required to keep details of the data they share, the reason for it, and the entities that they share with. This should form part of their records under the DPA provisions.

Safe Harbour provision

34. We have provided an explicit mechanism that allows regulated sector entities to share data between themselves and with law enforcement. The model is outlined below.

Basis for sharing

35. Information may be shared either:
 - a. following a request to share information between regulated sector entities by the NCA, or
 - b. following an entity in the regulated sector having formed a suspicion about a client in relation to money laundering deciding to share data with another company for the purpose of preparing a more detailed report in relation to the suspicious activity of the client.

Protection for data sharing

36. Any such disclosure:
 - a. is deemed not to breach the DPA;
 - b. does not give rise to any other form civil liability (including ensuring the provisions are sufficient to address the Tournier principles); and
 - c. does not amount to an offence of “tipping off” pursuant to s.333 of POCA.
37. Where such voluntary sharing takes place, the sender will be exempt from any subsequent data subject access request made pursuant to sch7 DPA, as amounting to a “crime and taxation” disclosure, therefore, absent a court order to the contrary, information and the fact that a disclosure has been made voluntarily, would not be subject to disclosure to the data subject. Furthermore, this would also act to take precedence above contractual obligations (with individual and commercial customers) and therefore preventing disclosure to the customer, in spite of any contractual provisions to the contrary.
38. The provision will only apply where the data was shared for the purpose stated above.

E. Appraisal (Costs and Benefits)

OPTION 2 – legislate

COSTS

39. There will be minimal one off familiarisation costs to the **regulated private sector** who wish to take part for establishing how to correctly share data under the mechanism. There will be ongoing gross costs for managing the information sharing process. Despite attempts at obtaining them, it has not been possible to obtain estimates for this cost from the sector. The legislation we are putting in place permits the voluntary sharing of personal data for the purpose of tackling money laundering and terrorist finance. The regulated private sector entities that will use this legislation will choose to do so on their initiative, and will accept the ongoing cost of doing so. There is therefore zero net cost.
40. The measure may yield more information submitted to law enforcement, potentially leading to new investigations. Any such investigations would be an **opportunity cost for law enforcement**, but would represent better user of time compared to the alternative, without the better insight gleaned from information sharing.

BENEFITS

41. The benefits for the private sector using the legislation will be that it will allow them to better identify the threat from money laundering and the individual(s) behind it, and take measures to inform the authorities and to protect themselves. The changes are part of the wider programme of work to reform the UK AML regime, and will operate alongside brought about through the delivery of the Action Plan for Anti-Money Laundering and Counter Terrorist Financing.

SMALL AND MICRO BUSINESS ASSESSMENT

42. Small and micro businesses make up the vast majority of the regulated sector by number of businesses, so may be affected by this measure. As for all businesses within scope, it would be for each entity to determine whether they wished to contribute information, and there would be no penalty if they declined. The measure would provide protection for small and micro businesses who wished to share information under the appropriate reasons to contribute to anti money laundering and terrorist finance law enforcement.

BUSINESS IMPACT TARGET

43. There is no additional direct cost on business, so the BIT score is 0.

F. Risks

OPTION 2 – legislate

44. The purpose of these provisions is that the risks of civil liability for sharing data are removed from the regulated sector, where they use the proposed changes to share data relating to suspicions of money laundering. The main risks are likely to be:
- a) That the regulated sector uses the proposed changes to share data for purposes other than tackling money laundering. Firms in the regulated sector are also subject to the requirements of the DPA, and can be audited for compliance.
 - b) That the regulated sector removes services from innocent individuals following the sharing of data. However, as the sharing of information should increase firms' collective knowledge of money laundering, this risk should be reduced, rather than increased, by the provisions in this Act.

G. Enforcement

45. This is a provision for voluntary sharing of data, and as such no specific enforcement requirements. The regulated sector will be expected to comply with its existing obligations in relation to the protection of data.

H. Summary and Recommendations

46. The table below outlines the costs and benefits of the proposed changes.

Option	Costs	Benefits
2	<p>There will be gross costs incurred by the regulated private sector for sharing data between themselves and with law enforcement. There will also be minimal familiarisation costs. However since this is a voluntary measure, it is assumed the benefits to the private sector would outweigh the costs.</p> <p>Law enforcement could face opportunity costs from investigation begun as a result of better intelligence.</p>	<p>Private sector are better able to identify the threat from money laundering and the individual behind it, and take measures to inform the authorities and to protect themselves</p>

47. The preferred option is option 2. It provides legal cover to allow private sector entities in the regulated sector to implement data sharing between individual institutions for the purpose of developing more detailed and accurate SARs, and to develop the ability to protect themselves.

I. Implementation

48. The powers will be commenced by order subject to operational needs and the passage of any necessary secondary legislation/publication of statutory guidance. Where appropriate, this will be on a common commencement date.

J. Monitoring and Evaluation

49. This is a voluntary measure, and formal monitoring is not seen as proportionate at this stage.

K. Feedback

50. Informal feedback will continue to be sought from stakeholders.