

Mr Roderick Macauley
Ministry of Justice
102 Petty France
London
SW1H 9AJ

24 March 2017

Dear Mr Macauley

CORPORATE LIABILITY FOR ECONOMIC CRIME: CALL FOR EVIDENCE

The Federation of Small Businesses (FSB) welcomes this opportunity to submit comments to the call for evidence on corporate liability for economic crime. FSB is the UK's leading business organisation. Established over 40 years ago to help our members succeed in business, we are a non-profit making and non-party political organisation that's led by our members, for our members.

Our mission is to help smaller businesses achieve their ambitions. As experts in business, we offer our members a wide range of vital business services, including advice, financial expertise, support and a powerful voice in government.

FSB is also the UK's leading business campaigner, focused on delivering change which supports smaller businesses to grow and succeed. Our lobbying arm starts with the work of our team in Westminster which focuses on UK and English policy issues. Further to this, our expert teams in Glasgow, Cardiff and Belfast work with governments, elected members and decision-makers in Scotland, Wales and Northern Ireland.

If you have any further questions regarding our views on this issue please do not hesitate to contact my colleague Richard Hyde on the following number: 020 7592 8127 or on his email address: Richard.hyde@fsb.org.uk

Yours sincerely

Richard Parlour
Chairman, FSB Home Affairs Committee

FSB response to Corporate Liability for Economic Crime: call for evidence

March 2017

CORPORATE LIABILITY FOR ECONOMIC CRIME: CALL FOR EVIDENCE

The Federation of Small Businesses (FSB) welcomes the opportunity to respond to the call for evidence by the Ministry of Justice (MoJ) on proposals for introducing corporate liability for economic crime on behalf of its members across the UK.

Introduction

FSB strongly supports the ambition of trying to reduce the significant levels of economic crime in and against the UK. Economic crime is costly for smaller businesses. It adds to the cost of doing business and impedes their competitiveness by negatively impacting their ability to invest, take on new staff and grow. For some, its consequences can be existential, resulting in their closure. The knock-on impacts of economic crime on the UK's economy is significant as it impedes the important role that small businesses play in driving market competition, innovating new products and services and generating employment.

Small business and economic crime

Data collected in a 2016 survey has enabled FSB to estimate the cost of both offline and online crime to the smaller business community in the UK and by extension to the UK economy. These estimates are set out in Box one below.

Box one: annual cost of crime to smaller businesses¹

In total:

- Offline crime costs smaller firms around £7.64 billion a year.
- Online crime costs UK smaller business £5.26 billion per annum.
- Together the annual cost of crime to the smaller business community is in the region of £12.9 billion a year.

The same survey highlighted significant numbers of smaller firms have been impacted by a number of specific types of offline and online economic crime (including different types of fraud and IP crime). Table one below outlines some of the most salient economic crime data captured from FSB members and provides estimates of the number of crimes in these categories impacting the smaller business community.

¹ FSB surveyed 1006 members in January 2016 about their experience of crime against their business interests. There were 5.4 million small and medium-sized businesses in the UK in 2015. All calculations are made on the basis of this number.

Table one: economic crime impacting smaller businesses in the UK - 2014 and 2015²

| Offline | Online |
|--|--|
| Fraud | |
| 9 per cent had suffered as a result of a fraudulent payment by a customer. | 10 per cent have been caught up in card not present fraud i.e. processing a fraudulent online payment. |
| 4 per cent of respondents had been impacted by identify fraud. | 3 per cent have been impacted by online invoice fraud. |
| 3 per cent had been impacted by fraud by an employee of some kind. | |
| IP crime | |
| 1 per cent had suffered as a result of counterfeiters selling their products unlawfully. | 3 per cent have suffered from online IP theft. |
| | 2 per cent have been impacted specifically by online corporate identity theft. |
| Approximate number of economic crimes impacting smaller business³ | |
| 918,000 | 972,000 |
| Combined total number of economic crimes impacting smaller businesses | |
| 1,890,000 | |

The data outlined in Table one illustrates that the categories of economic crime most heavily impacting smaller businesses are fraud and IP crime. Within these categories fraudulent payment and card-not-present (CNP) fraud stand out as the most frequently highlighted types of economic crime impacting smaller businesses. Taking all the types of fraud and IP crime reported by FSB members as impacting them together suggests that smaller businesses across the UK were impacted by nearly 2 million frauds and IP crimes of various kinds in 2014 and 2015.⁴

² 1006 FSB members were surveyed in 2016 and were asked about their experience of crime against their business interests over the period 2014 and 2015.

³ The calculation assumes that each victim is only a victim once. Whereas, in reality many businesses are likely to be victims more than once. The 2016 FSB survey into crime against smaller business found that typically smaller businesses were the victims of some sort of cyber crime four times and an offline crime three times over the years 2014 and 2015.

⁴ It is worth noting, to help provide an idea of the scale of economic crime against smaller businesses highlighted in the FSB data compared to that captured by official statistics, that:

- The ONS reported in 2016 that in the preceding 12 months there had been 3.6 million fraud offences in the UK.
- The National Fraud Intelligence Bureau (NFIB) recorded 622, 729 frauds between October 2015 and September 2016. NFIB in particular appears too significantly under record the incidents of fraud in the UK.

Source: ONS. 'Crime in England and Wales: year ending September 2016'. (2017). Available at:

<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016>

ONS. 'Crime in England and Wales: Bulletin Tables'. (2017) Available at:

<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesbulletintables>

Around 0.4 per cent of frauds result in a criminal sanction.⁵ This very low level of effective enforcement of the law against fraud highlights the degree to which much more could and needs to be done by the authorities to tackle this highly detrimental crime. Overhauling the corporate liability regime in the ways suggested in the call for evidence is unlikely to do much to deal with the large problem of economic crime (highlighted in Table one) perpetrated against smaller businesses by criminals.

Big gains will accrue to the economy as a result of dealing with the significant number of incidents of economic crime against the small business community. A lower cost of crime would enable smaller businesses to get on with investing, innovating and generating employment. In order to substantially reduce the levels of economic crime against smaller businesses the enforcement response by the authorities needs to be considerably improved.

The consequences for small businesses of the Ministry of Justice proposals

FSB believe the proposal to place criminal liability on anyone other than those that have committed the crime, conspired in its formulation or assisted with its commission is one fraught with risks. It could end up being a counter-productive undermining the fight to reduce the significant volume of economic crime committed against smaller businesses. As a result, FSB has a number of specific concerns about the proposals in the call for evidence, which are set out below.

The risk of injustice is greater than the potential benefits

Being held criminally liable for an action you have not committed or been purposefully involved with, in some form, is an approach to be utilised sparingly and only where the case for doing so is overwhelming because of the high risk of injustice associated with it.

There are a range of alternative measures to those proposed in the call for evidence which are likely to be as, if not more, effective in dealing with economic crime. These alternatives do not carry the same risk of injustices associated with the corporate criminal liability approach occurring.

Consequently, FSB consider that the strong case required to justify the type of change proposed by MoJ in the call for evidence has not been made given the considerable risk to smaller businesses of numerous instances of injustices in comparison to choosing a range of alternate policy options which, in the long-run, have the further advantage of being more effective at reducing levels of economic crime, especially against smaller businesses.

Adding to the regulatory burden for small businesses

The criminal liability proposals will mean small businesses face new regulatory risks. These inevitably come with associated costs. Operating a small business will become more

⁵ Button, M et al. 'Fraud and Punishment'. (2012). Available at: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/fraud-and-punishment.pdf>

complicated. The costs of running a business will increase as a result of the proposed new liabilities. At the same time, it will do little to deal with the work of organised fraudsters and IP thieves that commit most economic crimes against smaller firms. The measures will impose additional administrative and compliance (i.e. regulatory) costs for little benefit. Consequently, for smaller businesses the proposals are disproportionate in the burden they will create when suitable alternatives which would achieve equally good if not better outcomes (and which have a lower burden for businesses) are not being pursued.

Small businesses do not have the resources or knowledge to devise and implement extensive formal anti-economic crime policies in order to minimise the risks associated with the new duties that will inevitably come with these proposals. Part of the increased burden that smaller businesses will incur as a result of the proposals will stem from the need for many businesses to buy-in advice and support from outside experts in order to put the policies and processes in place to try and ensure they could robustly defend themselves against any possibility of a successful prosecution.

These proposals will increase the risks for smaller businesses associated with taking on or increasing their workforce. Recruiting employees or engaging with new contractors are likely to mean additional risk as a result of these proposals. Adding further risk to what is already, for smaller businesses, a step fraught with (considerable) risks will dis-incentivise the expansion of a business's workforce. There are potentially similar incentive implications for small businesses in relation to engaging with new contractors. The long-run result will be lower levels of employment and a mis-allocation of labour away from where it is most productively employed. These employment and inefficiency consequences need to be reflected fully in the Impact Assessment and factored into the decision making over whether the wider impacts of the proposals are worth the costs that will come along with taking them forward when other measures may deliver equally good, if not better, outcomes in the longer-term.

Finally, in many small businesses it will be difficult for an employee to commit crimes because of the intimate nature of working in a small workforce, which reduces the opportunities for illicit activity. However, in those circumstances where wrongdoing is suspected by the business owner/ manager the result of the MoJ proposals could be greater reluctance to report any suspicions to the police. The current inconsistent response to crime by the police puts business owners off reporting incidents as it is.⁶ This measure could further dis-incentivise reporting of fraud and other economic crimes by increasing the risks associated with doing so. At the very least, creating a law which results in greater reluctance to report crime will negatively impact the ongoing construction (by the police and others) of an accurate intelligence picture of local, regional, national and international economic crime.

⁶ FSB research found that: 24 per cent of members do not report any crime against their business, while a further third (33%) only report the most serious crimes. The reasons behind not reporting crimes revealed a high degree of fatalism about the effectiveness of the criminal justice system to respond. 47 per cent of those who did not report a crime or only reported the most serious ones reported that they did not report crimes because they felt that there would be no point because 'nothing would be achieved' by the police in doing so.
Source: 'FSB.' Business Crime Survey'. (2016).

Specific risks as a result of card-not-present (CNP) fraud

FSB has particular concerns that small businesses, especially retailers, may end up criminally liable for processing fraudulent card payments as a result of the proposals. This would be a counter-productive and unfair consequence if that was to be the case.

Around 10 per cent of FSB members have unwittingly been involved in CNP fraud. The proportion doubles for those businesses in the retail and wholesale sectors to 21 per cent. Across the small business population of the UK, this suggests that there are approximately at least 540,000 incidents of CNP fraud, over a two-year period, which small businesses innocently get caught up in.⁷

Consequently, FSB would like clarity on whether, for example, adhering to PCI DSS will qualify as a defence against a criminal charge?⁸ The bureaucracy associated with PCI DSS is already onerous for small businesses and the banks frequently 'charge back' to the merchant the cost of the fraudulent transaction i.e. shift the loss onto the retailer.⁹ Changes which brought in corporate liability could see more small businesses at risk of criminal prosecution for innocently processing such transactions. Changes along the lines proposed in the call for evidence can only be justified if a number of the other risks and costs that small businesses bear due to CNP fraud are substantially reduced. Government would need to make sure:

- There is an effective system in place which reduces significantly the chances of a small business processing a fraudulent claim. This would require the banks and card companies operating an efficient and timely system for blocking stolen or cloned cards/ card details.
- Small businesses are relieved of much of the bureaucracy and burden associated with PCI DSS.
- Banks are prevented from 'charging back' fraudulent losses to the merchant.

The process for creating new criminal offences

The proposal that additional 'economic offences' could be added to the list to which this new measure could apply through secondary legislation is concerning. Criminal liability can result in the imprisonment (deprivation of liberty and sometimes property) of business owners. There would certainly be a negative impact on the income of the small business with potential knock-on consequences for employees and families as well as suppliers and customers in commercial relationships with the accused business. Therefore expansions in the scope of this law should be made with the full scrutiny of Parliament. Such measures should not be pushed through without thorough consideration and the full approval of MPs who are in-turn accountable to the electorate for their decisions. It is only in these circumstances that the small business community can have confidence in the legitimacy of

⁷ The calculation was made assuming that the 10 per cent of members reporting being caught-up in a CNP fraud were only caught out once. In reality, some are likely to have been caught put several times over the two years, 2014 and 2015.

⁸ https://www.pcisecuritystandards.org/pci_security/

⁹ FSB. 'Cyber security and fraud: the impact on small businesses'. (2013).

new criminal offences which put them under the threat of criminal sanction and could result in them being arrested and prosecuted.

Measures to reduce the quantity of economic crime

We consider that, for small businesses, this consultation is something of a missed opportunity. Given the scale of economic crime against small businesses outlined above this could have been a chance to develop a cross-government strategic approach to dealing with economic crime, taking in the full panoply of relevant departments and enforcement agencies.

A more holistic approach to dealing with economic crime, and one that avoided many of the likely negative consequences that the corporate liability proposals will result in for smaller businesses, would be based on four pillars. These pillars need to be developed and implemented in a co-operative and co-ordinated way, not just between different parts of government but between the many agencies and individuals involved in enforcement both domestically and internationally. The private sector is where the majority of the preventative capacity against crime exists. It is also the source of most of the intelligence needed to tackle economic crime. Therefore it needs to be a central part of any plan too. Finally, the system needs to be adaptable so that it can change in the face of the complex and evolving threat from economic crime.

The four pillars of a holistic approach should be:

- **Knowledge:** a substantial improvement in efforts to increase the knowledge and levels of awareness among the small business community about the threats to their business from economic crime in general and fraud in particular and the appropriate counter-measures that businesses can take to reduce their risk.¹⁰
- **Information:** the development of national information sharing measures which can deliver useable information to small businesses about 'real-time' threats to help increase levels of prevention. An option for improving the quality and increasing the quantity of available information about fraud threats in particular could be to borrow the principle of the mandatory reporting requirements found in the Anti-money Laundering (AML) regime and applying it to fraud. The potential role of incentives for encouraging the reporting economic crime should be looked at. Rather than offering the prospect of prosecution if a small business owner reports an economic crime in their business against others a more fruitful approach would be to provide support and a degree of 'safe harbour' to incentivise openness and co-operation.
- **Security:** building robust anti-fraud measures into infrastructure whether that be technological or economic. This should include:

¹⁰ This could start with more efforts to highlight the existence and role of Action Fraud. FSB called for more to be done to raise its profile among the small business community in our 2013 report on cyber crime and fraud: FSB. 'Cyber security and fraud: the impact on small businesses'. (2013).

- Financial intermediaries taking more responsibility to help identify and prevent fraud in particular but also other economic crimes where possible.¹¹
- Building in more anti-crime measures by design.¹²
- **Enforcement:** an adequate investigatory and law enforcement response i.e. sufficiently well-resourced, organised in the most effective way and capable of dealing with the scale of the problem. At the most basic level the significant decline in fraud specialists in police forces across the country over recent decades has been particularly detrimental to effective action against fraudsters.¹³ In addition, the myriad public enforcement bodies that can investigate and enforce the law against various kinds of economic crime along with divergent legal frameworks for these bodies is detrimental to co-ordination and co-operation.¹⁴ Further, to maximise enforcement capacity and capability public efforts should be complemented with more private enforcement action (both criminal and civil). Ways of incentivising more of it should be identified through a review of the framework governing the current scope and incentives for private enforcement action.¹⁵ More consideration should be given to how existing civil sanctions might be better used and whether new or enhanced existing options might be helpful for dealing with economic crime. Accompanying a specific look at the civil framework should be the establishment of a periodic review of the entire criminal and civil legal framework pertaining to economic crime.¹⁶ Much economic crime is cross-border and the channels for international co-operation should be bolstered where possible e.g. streamlining and strengthening Mutual Legal Assistance Treaties (MLATs) and the terms of inter-agency Memorandums of Understanding (MoU) and Service-level-agreements (SLA). The right long-term funding, strategic, organisational, technological and operational response needs to be accompanied by a swift and dissuasive punishment framework against those committing

¹¹ Improving the incentives for those providing the economic infrastructure for the UK (e.g. banking and payment services) to take the most effective action to reduce fraud in particular would significantly help in the fight against fraud.

Source: FSB. 'Cyber Resilience: how to protect small firms in the digital economy'. (2016).

¹² FSB. 'Cyber Resilience: how to protect small firms in the digital economy'. (2016).

¹³ Button, M et al. 'Fraud and Punishment'. (2012). Available at: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/fraud-and-punishment.pdf>

¹⁴ As has been noted by Jonathan Fisher QC, in relation to fraud: '*The haphazard development of the Government agencies tasked with tackling these crimes has created a system of overlapping responsibilities for investigation and prosecution, a dispersion of powers and caused unnecessary duplication of manpower and specialist resources*'. Further: '*As if this intricate web...[of agencies]...wasn't complicated enough, these agencies all operate under differing statutory frameworks, further exacerbating the problem*'.

Source: Fisher, J. 'Fighting Fraud and Financial Crime: A new architecture for the investigation and prosecution of serious fraud, corruption and financial market crimes'. (2010).

¹⁵ A review of the legal, organisational and resource landscape to identify barriers to leveraging in more private activity against fraud was mooted by FSB in its report 'Cyber Resilience: how to protect small firms in the digital economy'. A number of promising ideas for helping achieve this end have been set out by Button et al in their report 'Fraud and Punishment'.

Sources: FSB. 'Cyber Resilience: how to protect small firms in the digital economy'. (2016) and: Button, M et al. 'Fraud and Punishment'. (2012).

¹⁶ In a 2010 research note for Policy Exchange, Jonathan Fisher QC outlined a number of reforms to aspects of the criminal law and procedure, beyond the imposition of corporate criminal liability, which would help in the fight against financial fraud e.g. the powers of the Crown Courts in relation to adjusting property rights and confiscation. Source: Fisher, J. 'Fighting Fraud and Financial Crime: A new architecture for the investigation and prosecution of serious fraud, corruption and financial market crimes'. (2010).

fraud and other economic crimes.¹⁷ This will require a significant firming up of the current sentencing framework for such crimes.

Perhaps the most important of the four pillars is the enforcement response. All relevant public enforcement agencies need adequate funds to deliver a step-change in the end-to-end response to economic crime. This will require considerable investment, sustained over a long period of time, in order to ensure:

- The authorities have adequate numbers of personnel.
- Personnel have the right skills i.e. are sufficiently trained.
- Any organisational change deemed necessary can be planned thoroughly and carried out effectively.¹⁸
- The most appropriate technology can be deployed by enforcement agencies and updated when required.
- There is the scope for leveraging in the right private sector expertise and capacity.
- Best practice can be swiftly developed and there are mechanisms for its rapid dissemination across public and private sector.
- There are the structures and tools in place to make international co-operation against economic criminals as seamless and efficient as possible.

Achieving the levels of capacity and capability needed to tackle the quantity of economic crime against small business and the UK economy will require the relevant law enforcement authorities to develop a long-term strategy which can be expected to be adequately funded by the government. The strategy should be developed primarily by the enforcement agencies along with the private sector input. The structural and operational aspects of the strategy need to be supported by an adequate legal framework. Government therefore also needs to commit to provide any amount of time necessary for required legislation. This law enforcement-led strategic approach is one FSB has argued for in relation to cyber crime too.¹⁹ With much economic crime being synonymous with cyber crime these strategies must be fully integrated with each other.

Taking the proposals forward

As the leading representative body of small businesses we intend to work constructively with Government, the police and other enforcement authorities to help tackle the growing threat of fraud and other economic crimes against small businesses and the economy. We would welcome the opportunity to talk in person to the Ministry of Justice about our concerns regarding the proposals for corporate criminal liability and explore a wide range of

¹⁷ 'To be effective in securing deterrence, sanctions must be: Inevitable and unavoidable; Administered speedily...[and]...Severe...In general these three observations do not apply in respect of criminal penalties against fraudsters. Non-criminal sanctions are currently underutilised'.

Source: Button, M et al. 'Fraud and Punishment'. (2012). Available at: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/fraud-and-punishment.pdf>

¹⁸ The role and effectiveness of Action Fraud in the fraud reporting and criminal intelligence landscape and its linkages to law enforcement is particularly ripe for re-examination.

¹⁹ FSB. 'Cyber Resilience: how to protect small firms in the digital economy'. (2016).



alternative ways that small businesses and the UK economy can be better protected from economic crime.