

Written evidence submitted by Dr Lorenzo Pasculli

Executive summary

I. Objectives

This submission assesses the Government's measures to

- A. Reduce the risk of people being taken advantage of by fraud at this time, in particular with regard to vulnerable groups;
- B. Ensure that businesses and individuals are claiming appropriately and that fraudulent claims within the Coronavirus Job Retention Scheme (CJRS) and the Self-employed Income Support Scheme (SEISS) are detected.

II. Findings

A. The response of Government and regulators to general coronavirus-related fraud risks is inadequate:

1. The information, guidance and advice publicly released is
 - a. fragmentary and difficult to access;
 - b. poorly coordinated;
 - c. incomplete or outdated.
2. An ambiguous statement released by the FCA can inadvertently encourage a relaxation of corporate controls on crime/fraud risks during the pandemic;
3. There are too many and confusing reporting channels;
4. Insufficient efforts are dedicated to tackling the root causes of fraud, which have been aggravated by the pandemic.

B. The Government's response to the specific fraud risks triggered by CJRS and SEISS is also inadequate:

1. The newly established COVID-19 Counter Fraud Response Team (CCFRT):
 - a. Lacks transparency/accountability;
 - b. Fails to address all relevant fraud risks;
 - c. Does not cover *ex-post* risk assessment mechanisms;
 - d. Fails to engage properly with the international community and academic experts.
2. The HMRC lacks the capacity to conduct effective audits;
3. Excessive reliance is placed on employee reporting, which places a considerable psychological burden on individuals;
4. Insufficient advice, support and mental care is provided to victims and whistleblowers.

III. Recommendations

1. Centrally coordinated and unified information website on fraud risks;
2. Extensive awareness-raising campaign also through press, radio and television;
3. Avoiding public statements that can discourage reporting and undermine controls;
4. Rationalisation/simplification of reporting channels through a centralised system;
5. Establishing a national authority for whistleblowers;
6. Improving the work of CCFRT by
 - a. making it more transparent;
 - b. expanding its focus to all relevant risks;
 - c. introducing *ex-post* risk assessment mechanisms;
 - d. expanding its international partnerships;
 - e. engaging with the academic community.
7. *Ex-ante* and *ex-post* crime risk assessments and crime proofing for any policy/regulation;
8. Establishing a national authority for disaster fraud.

Full submission

1. Overview

1.1. Brief introduction

I am submitting this evidence in a personal capacity, as an academic expert in financial crime. I am the [Associate Head for Research at Coventry Law School and an Associate at the Centre for Financial and Corporate Integrity at Coventry University](#).

My research combines findings from criminology, sociology, law and psychology to understand the causes of financial crime and develop measures to effectively prevent and counter it.

1.2. Reasons for the submission and focus

I am submitting this evidence to support with my expert knowledge an impartial assessment of the Government's response to coronavirus-related fraud risks and identify effective ways to improve it.

This submission addresses the following terms of reference:

- a. **Support to businesses and Financial services:** What are the financial regulators and the financial sector doing to reduce the risk of people being taken advantage of by fraud at this time, in particular with regard to vulnerable groups? (Para. 2 below)
- b. **Job Protection Scheme and Self-employment Income Support Scheme:** Is the Government doing enough to ensure that businesses and individuals are claiming appropriately and that fraudulent claims are detected? (Para. 3)

The research in this submission has neither been published nor submitted for publication elsewhere.

2. The Government's response to COVID-19 fraud risks

2.1. Awareness-raising and public information

Various government bodies have published information and guidance on COVID-19-related fraud risks aimed at the general public and businesses. Unfortunately, such awareness-raising campaign is far from ideal.

- 1) **Fragmentariness and limited accessibility.** The information and guidance released by government agencies are scattered throughout more than 20 different webpages, of which 5 included in the gov.uk website (e.g. [Guidance. Fraud control in emergency management](#); [Advice on how to protect yourself and your business from fraud and cyber crime](#); [Coronavirus \(COVID-19\)](#));

[increased risk of fraud and cybercrime against charities](#); [Be vigilant against coronavirus scams](#); [Genuine HMRC contact and recognising phishing emails](#)), and many others contained in the websites other government agencies (e.g. [CPS](#), [FCA](#), [National Crime Agency \(NCA\)](#), [NHS](#), [National Trading Standards \(NTS\)](#), [National Cyber Security Centre \(NCSC\)](#), [The Pensions Regulator](#), [Action Fraud](#), [Take Five](#) and [Friends against Scam](#)). Moreover, most County councils, City councils and police forces have released their own advice in their institutional websites. While a certain level of diversification is required to address different fraud risks and different sectors, the unnecessary multiplication and complexity of online sources of guidance and information make it difficult to access and understand. Moreover, the choice of the Internet as the primary (if not only) means of information is debatable as not everyone, and especially vulnerable groups, can easily access it or use it properly. I could find no evidence of information campaigns launched through other media (press, television and radio).

- 2) **Lack of coordination.** The various sources of advice are not appropriately coordinated. The information provided differs from one website to another, and so does its format. Some websites are very specific, others are more generic. Many sources do not follow the general 'Stop, Challenge and Protect' approach adopted by the Government (e.g. in the [gov.uk](#) and [Action Fraud](#) websites). The Cambridgeshire County Council [webpage](#) even refers citizens to the advice provided by the website [Which?](#), which is not backed or checked by the Government and offers commercial products and services. Different sources suggest different reporting channels. The [Suffolk County council website](#), for instance, does not advise to report fraud cases to Action Fraud, but only to call National Citizen's Advice helpline.
- 3) **Missing/outdated information.** Some online advice is incomplete and out of date. Some gov.uk webpages are months old – e.g. the [Advice on how to protect yourself and your business from fraud and cyber crime](#) dates back to 27 April 2020. No relevant agency has published informative videos on COVID-19-related fraud risks. The latest video uploaded on YouTube by Action Fraud is 10 months old, the latest uploaded by Friends against Scam 1 year old, while the latest uploaded by Financial Fraud Action UK is 2 years old. Some websites include broken links to other webpages: the [Staffordshire County council website](#), for instance, includes a [wrong link](#) to Take Five's advice. Other sources don't cover important fraud risks. The NHS's [COVID-19 counter fraud guidance](#) is mostly addressed to NHS staff, rather than the general public and it does not mention the risks of fraud related to the new 'Test and Trace' system flagged by the [Local Government Association](#). Such risks are briefly mentioned in the general ['Test and Trace' webpage](#) but no extensive advice is provided.

2.2. Advice/support to business

The advice to business is overall more effective than those to private citizens. The NCSC has published a good [Guidance on Home Working](#) including useful references and a clear [infographic](#). The FCA's webpage [Avoid coronavirus scam](#) is

also effective and contains links to helpful tools, such as the [Financial Services Register](#), the [Warning List](#) and [ScamSmart](#).

However, an [online message published by the FCA](#) can inadvertently undermine control measures during the pandemic. After reiterating that ‘firms should not seek to address operational issues by changing their risk appetite’, the FCA recognises that ‘firms may need to re-prioritise or reasonably delay some activities’, including ‘customer due diligence reviews, or reviews of transaction monitoring alerts’. This would be considered ‘reasonable’ by FCA as long as ‘the firm does so on a risk basis’ (e.g. not for high-risk activities, such as terrorist financing) and plans to return to the business as usual review process as soon as possible. Such ambiguous wording can encourage a relaxation of controls on crimes and frauds that might not be considered such ‘high’ risks as terrorist financing, but can still cause considerable harm to private customers and vulnerable individuals.

2.3. Reporting, investigation and prosecution

The Crown Prosecution Service (CPS) has [prioritised the prosecution of all COVID-19-related cases](#), including fraud and dishonesty offences against vulnerable victims and the [SFO is continuing its investigations](#). Despite such prioritisation, a major obstacle to effective prosecution can come from too many reporting channels, including:

- [Action Fraud hotline and online reporting tool](#)
- Citizens Advice
- NCSC’s report@phishing.gov.uk
- FCA’s [Consumer Helpline](#) or online [reporting form](#)
- [SFO online reporting form](#)
- HMRC’s various [reporting channels](#)
- The long and confusing [list of prescribed entities for whistleblowing](#)

It can be difficult – particularly for vulnerable citizens, such as the elderly, or those with limited access to or experience of the Internet – to identify the right reporting channel. As a result, additional time and resources must be spent to redirect the victim towards the appropriate channel with possible delays in investigations.

Moreover, some of these channels are providing a reduced service. [Action Fraud’s website](#) states that ‘Due to the ongoing COVID-19 situation, unfortunately our contact centre is currently providing a reduced service. If you do need to chat to us, we have a small number of advisors on hand to help but please be advised that waiting times will be longer. We apologise for any inconvenience caused. If your UK business, charity or organisation is currently under cyber attack and data is potentially at risk please call 0300 123 2040 immediately and press 9. You can continue to make reports of fraud in the normal way via the website.’ Such a message can:

- a) encourage fraud;
- b) discourage reporting;
- c) create a disparity of treatment between individuals and organisations, reflecting the assumption that the interests of the latter are valued more than the former’s;

- d) foster frustration and social mistrust.

2.4. *Lack of focus on root causes*

A worrisome shortcoming of the Government response is the lack of focus on the root causes of fraud. While it is understandable that in the emergency of the pandemic the Government adopts immediate action to address urgent practical issues, there is no reason to ignore the social and human factors that can trigger criminal motivations. In fact, the pandemic has aggravated some of the factors, such as social and economic inequality ([Adams-Prassl et al, 2020](#)), that typically cause psychological pressures that can drive individuals to crime ([Pasculli, 2020a](#)).

The Government is responding to these strains mainly through financial support schemes such as CJRS and SEISS, but this is insufficient, while broader social interventions are lacking. The major shortcoming of this strategy is that the Government is failing to notice that it is precisely the focus on financial gain and opportunity that motivates fraudsters and other financial criminals – rarely driven by poverty, but more often by greed and/or unreasonable expectations ([Pasculli, 2020a](#)). A research-based comprehensive strategy, coordinated at a national level, bringing together welfare measures, mental care, education, and community action is required to promote, both in individuals and organisations, a culture of honesty, solidarity and legality to counter opportunistic, profit-oriented mindsets that can motivate fraudulent behaviours ([Pasculli, 2020a](#)).

3. The Government's response related to the Coronavirus Job Retention Scheme (CJRS) and Self-employment Income Support Scheme (SEISS)

3.1. *Risk assessment and management: the COVID-19 Counter Fraud Response Team (CCFRT)*

To help the public sector understand its fraud risks – especially those generated by stimulus spend – and design adequate countermeasures, the Cabinet Office's centre of the Counter Fraud Function has established the COVID-19 Counter Fraud Response Team (CCFRT). The risk-based approach adopted by CCFRT is promising and welcome. Research from various disciplines demonstrates that [policy and regulation can inadvertently create or increase crime risks](#) and suggests that systematic crime [risk assessment mechanisms of proposed policies and regulation \(so-called 'crime proofing'\) can help mitigate such risks](#) (Albrecht et al., 2002; Savona et al., 2006; Savona, 2016; Caneppele et al. 2013; Hoppe, 2014; Pasculli, [2017a](#), [2017b](#), 2019, 2020b). Nevertheless, CCFRT has many shortcomings.

- 1) **Lack of transparency and accountability.** It is very difficult to assess CCFRT's work as few sources about it are publicly available. CCFRT does not have a dedicated webpage and the only information accessible online is included in a handful PDF documents scattered in various random websites (e.g. [gov.uk](#), the [Mersey Internal Audit Agency \(MIAA\) NHS's website](#), the

[British Vehicle Rental & Leasing Association \(BVRLA\)'s website](#)). One of these [documents](#) claims that CCFRT 'have built an expert team who can provide a variety of expertise', but there is no indication of who these experts are, what their background is and how they were appointed. The [first issue of a newsletter \(April 2020\)](#) can be found in the MIAA/NHS website, but there is no trace of further issues. The lack of transparent information prevents full, impartial scrutiny by independent experts, relevant stakeholders and the general public, reduces the opportunities for improvement and prevents the dissemination of good practices beyond the public sector.

- 2) **Limited focus.** CCFRT's work focuses especially on protecting public money, rather than protecting businesses and individuals from other fraud or crime risks caused by financial support schemes. The [Counter Fraud Measures Toolkit](#) released by CCFRT suggests various due diligence measures, such as identity and account verification, to avoid irregular payments, but fails to address the risk that scammers [exploit support schemes to try to steal money from people](#) – as it happened in the [recently uncovered](#) scam designed to steal personal and financial details of millions of self-employed workers through fake HMRC text messages and website.
- 3) **Lack of ex-post evaluation.** The measure to assess and control fraud risks suggested by the [Counter Fraud Measures Toolkit](#) cover the design and implementation phase. A systematic mechanism to assess the crime and fraud risks actually triggered by each government policy and scheme after their termination is missing. *Ex-post* assessments are fundamental to learn from past mistakes and avoid repeating them – that is, to become acquainted with risks that had not been anticipated in the design and implementation stages and be able to address them in future policymaking (Pasculli, 2017).
- 4) **Limited international engagement.** CCFRT claims to use 'intelligence and analytics' from partnerships with Five-Eyes countries. These are the members of the [Five Eyes Intelligence Oversight and Review Council \(FIORC\)](#) and the [International Public Sector Fraud Forum \(IPSFF\)](#): the UK, Australia, Canada, New Zealand, and the US. It is unclear why CCFRT should circumscribe its international partnerships to such five countries. Surely intelligence from other (and closer) jurisdictions, such as European states, and international organisations, such as the European Anti-Fraud Office (OLAF) can be equally important.
- 5) **No engagement with scientific research.** CCFRT also claims to use intelligence from partnerships with the public and private sectors. Yet there is no evidence of engagement with scientific research and academia. CCFRT's [Counter Fraud Measures Toolkit](#) does not rely on the findings of previous research on crime risk assessment of policy and regulation. Instead, it is largely based on IPSFF's [Principles for Effective Fraud Control in Emergency Management and Recovery](#) – which doesn't refer to academic literature at all. There is no evidence of any involvement of academics in the work of CCFRT. Some of the above shortcomings could have been avoided by consulting academic experts.

- 6) **A missed opportunity?** Currently, CCFRT focuses primarily on stimulus spending, but [crime and fraud risks can be triggered by all sorts of government policies and schemes](#) (Albrecht et al., 2002; Savona et al., 2006; Pasculli, 2017a, [2017b](#), 2019, 2020b). The Government should consider expanding the remit of CCFRT so as to extend its risk assessment and management practice to every policy area.

3.2. Reporting, investigation and sanctions

HMRC is responsible for investigating cases of irregular CJRS and SEISS payments and [can audit retrospectively any claim](#). To facilitate this, HMRC has instituted a specific online form to [report HMRC-administered coronavirus \(COVID-19\) relief scheme fraud](#) and has [urged anyone concerned that their employer might be abusing the scheme to report them](#). More recently, facing increasing numbers of reports ([almost 1900 as of 29 May 2020](#)), the Government has proposed [amendments to the Finance Bill 2020](#) to give HMRC new powers to recover irregular payments and impose penalties for those who make deliberately incorrect claims and fail to notify the HMRC within 30 days.

There are various problems with this approach.

- 1) **Lacking capacity for random audits.** The [sheer volume of demand attracted by Scheme](#) together with the [capacity constraints](#) created by its implementation makes effective and extensive preventive auditing improbable and costly, meaning that most investigation will have to be retrospective ([Duncan and Lord, 2020](#)).
- 2) **Excessive reliance on employee reporting.** Despite the number of reports received by HMRC so far, researchers suggest that many cases could go unreported due to the many barriers to individual reporting ([Duncan and Lord, 2020](#)). Furloughed employees might feel ['blackmailed into working' and fear to lose their job by not doing so](#) or by reporting the company. Even if anonymity was assured, employees might refrain from reporting for fear that the withdrawal of government funding or the imposition of sanctions might put their company out of business ([Duncan and Lord, 2020](#)) or [force it to stop paying their colleagues](#).
- 3) **Insufficient advice and support.** Many of the above-mentioned barriers to whistleblowing can affect the mental wellbeing of employees. HMRC encourages reporting, but there is no evidence of any special advice or care measures to support employees victimised by furlough frauds or those who have reported their employees.

4. Recommendations

I suggest the following measures to remedy the above shortcomings.

A. Awareness-rising/Public information

- 1) Any information, guidance and advice on COVID-19-related fraud risks issued by national and local government agencies should be coordinated and accessible through one comprehensive and constantly updated online portal to avoid unnecessary repetitions, confusion and multiplication of sources. The portal should provide any advice relevant at a national level and across any sector, while it should refer to other agencies' website for sector-specific advice. An example of a centralised information portal is provided by the US [centralised coronavirus information website](#).
- 2) Information and guidance should not only be provided online but also through extensive campaigns via more traditional media, such as newspapers, radio and television, to the benefit of the elderly and other groups who might be unable to access the Internet.

B. Corporate controls/compliance

- 3) Governmental agencies and regulators should refrain from publishing ambiguous messages that can inadvertently discourage reporting, encourage a relaxation of corporate crime controls or fuel criminal motivations.

C. Reporting

- 4) Reporting channels should be rationalised. There should be a central national online portal for those who wish to report any kind of fraud. The portal could include a preliminary questionnaire relying on AI to direct the applicant to the appropriate authority according to the type of fraud to be reported (Action Fraud, HMRC, FCA, SFO etc). This centralised system could be used also to receive reports of misconduct from whistleblowers. A similar, although pretty basic, [online questionnaire is incorporated in the SFO website](#).
- 5) A national whistleblowers authority should be established to coordinate and provide guidance to prescribed entities, act (at least) as last-resort reporting channel when other channels prove ineffective, conduct investigation on reported wrongdoing, as well as regulatory and investigative failures by relevant organisations, and provide whistleblowers with appropriate advice and support (also psychological). The [US Office of the Whistleblower](#), the [Dutch Whistleblowers Authority](#) are examples of such institutions.

D. Crime risk assessment of policy and regulation

- 6) CCFRT should be improved as follow:
 - a. Its work should be better publicised, possibly through a dedicated website and by making any relevant policy document (newsletter, toolkits etc) released by the Team publicly available online to allow thorough public scrutiny and continuous improvement through external feedback;

- b. The focus of CCFRT should be expanded so as to cover not only risks of irregular payments of public money but, more broadly, any risk of harm caused to the public sector, as well as to private individuals and organisations, by frauds related to any other government policy/scheme;
 - c. *Ex-post* risk assessment mechanisms should be introduced to understand the risks created by government policies that had not or couldn't be foreseen during the design and implementation stages;
 - d. The work of CCFRT should benefit from broader international partnerships (beyond the Five-Eyes);
 - e. CCFRT's work should be based on scientific research and rely on continuous engagement with the academic community.
- 7) Given that any government policy and regulation can inadvertently create/increase risks not only of fraud but of [any other crime](#), the Government should take advantage of CCFRT's experience to start establishing permanent mechanisms to perform a thorough crime risk assessment of policy and regulation before and after their adoption and to adopt appropriate measures to control such risks.

E. National disaster fraud authority

- 8) The Government could also consider establishing (or developing CCFRT into) a national coordinating authority dedicated to improving the detection, prevention, investigation, and prosecution of criminal conduct related to natural and man-made disasters and other emergencies, such as the coronavirus, similar to the US [National Centre for Disaster Fraud \(NCDF\)](#).

References

Adam-Prassl, A., Boneva, T., Golin, M. and Rauh, C. (2020). 'Inequality in the Impact of the Coronavirus Shock: New Survey Evidence for the UK'. *Cambridge-INET Working Paper Series*. 2020/10. *Cambridge Working Papers in Economics*. 2023. Available from: <https://www.repository.cam.ac.uk/bitstream/handle/1810/305395/cwpe2023.pdf?sequence=1> [Accessed 25 June 2020].

Albrecht, H.-J. et al. (eds) (2002). *Criminal Preventive Risk Assessment in the Law-Making Procedure*. Freiburg im Bg: Max Planck Institute for Foreign and International Criminal Law.

Caneppele, S. Savona, E.U. and Aziani, A. (2013). *Crime Proofing of the New Tobacco Products Directive*. Trento: Transcrime-Università degli Studi di Trento.

Duncan, P. and Lord, N. (22 June 2020). 'Furlough, fraud and the Coronavirus Job Retention Scheme'. *Policy@Manchester Blogs*. <http://blog.policy.manchester.ac.uk/posts/2020/06/furlough-fraud-and-the-coronavirus-job-retention-scheme/> [Accessed 25 June 2020].

Hoppe, T. (2014). *Anti-Corruption Assessment of the Laws (“Corruption Proofing”)*. *Comparative Study and Methodology*. Sarajevo: Regional Cooperation Council.

Pasculli, L. (2017a). ‘*Corruptio Legis: Law as a Cause of Systemic Corruption. Comparative Perspectives and Remedies also for the Post-Brexit Commonwealth*’, *Proceedings of 6th Annual International Conference on Law, Regulations and Public Policy (LRPP 2017)*, 5-6 June 2017, Singapore. Singapore: GSTF. 189-197. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216442 [Accessed 25 June 2020].

Pasculli, L. (20 December 2017b). ‘How the law itself can be a corrupting, criminal force – and what can be done about it’. *The Conversation*. Available from: <https://theconversation.com/how-the-law-itself-can-be-a-corrupting-criminal-force-and-what-can-be-done-about-it-85287> [Accessed 25 June 2020].

Pasculli, L. (2019). ‘Seeds of systemic corruption in the post-Brexit UK’, *Journal of Financial Crime*. 26(3), pp. 705-718

Pasculli, L. (2020a). ‘The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory’. *Journal of Ethics and Legal Technologies*. 2(1), 48-74. Available from: <https://jelt.padovauniversitypress.it/system/files/papers/JELT-02-01-03.pdf> [Accessed 25 June 2020].

Pasculli, L. (2020b). ‘Foreign Investments, the Rule of Corrupted Law and Transnational Systemic Corruption in Uganda’s Mineral Sector’. In: R. Leal-Arcas (Ed.), *International Trade, Investment and the Rule of Law*. Chişinău: Eliva Press. 84-110.

Savona, E.U. (2016) ‘Proofing Legislation against Crime as Situational Prevention Measure’. In: B. Leclerc and E.U. Savona (eds.) *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiatives*. Springer 2016. 247.

Savona, E.U. et al. (2006). Double thematic issue *Proofing EU Legislation Against Crime*. *European Journal on Crime and Policy Research*. 12(3-4).

June 2020