Daylight Robbery

Policy Exchange

Uncovering the true cost of public sector fraud in the age of COVID-19

By Richard Walton, Sophia Falkner and Benjamin Barnard

Daylight Robbery

Uncovering the true cost of public sector fraud in the age of COVID-19

By Richard Walton, Sophia Falkner and Benjamin Barnard

Policy Exchange

About the Authors

Richard Walton served as a police officer in the Metropolitan Police in London for thirty years (1986-2016). A former Commander at New Scotland Yard, he was Head of the Metropolitan Police Counter Terrorism Command (SO15) between 2011-2016. He is now a Senior Fellow at Policy Exchange and a Distinguished Fellow at the Royal United Services Institute (RUSI). He holds a BSc Hons degree in Policing and Police Studies from Portsmouth University and a MSc in International Relations from the London School of Economics and Political Science (LSE).

Sophia Falkner is a Research Fellow at Policy Exchange. As part of the Liveable London unit, her main focus is on developing policy solutions for the everyday challenges faced by those who live and work in our capital city. She joined Policy Exchange in 2019 after graduating from the London School of Economics with a BSc in Economic History with Economics. At Policy Exchange, Sophia has contributed to 'Rekindling British Policing' (2019) and 'The First Hundred Days' (2019). Sophia has previously worked for a financial advisory firm in London and a think tank in Berlin.

Benjamin Barnard is Head of Technology Policy. He leads Policy Exchange's research into Technology and the Digital Economy. He joined Policy Exchange in July 2019 after graduating from Christ Church, Oxford with a First Class degree in History. He is the author of 'FinTech For All' (2020), which demonstrated how innovations in financial technology can improve access to banking, credit, insurance and debt advice services.

Published by
Policy Exchange, 8 – 10 Great George Street, Westminster, London SW1P 3AE

www.policyexchange.org.uk

ISBN: 978-1-913459-33-8

Contents

Foreword

The Rt Hon. the Lord Blunkett
Former Home Secretary (2001-5)

This publication is both timely and a reminder that at moments of great stress, those with evil intent take every opportunity to exploit the vulnerabilities of organisations and individuals. Historically, this was true at times of war, as it is today with the Covid pandemic.

Whilst many preach "sweetness and light", others dip below the radar in order to be able to take advantage of unusual and unforeseen circumstance, and bank on attention and resources being focused elsewhere.

This paper is of particular interest to me as I became interested in cybercrime way back when I was Home Secretary between 2001 and 2005. Both the extent and the potential for fraud online has grown exponentially over the last 15 years to a point where businesses, but also public services, need to treat the potential attack and fraud that accompanies it, as one of their highest priorities.

It is just at the moment when Government, by necessity, takes the lead in mobilising the nation that the potential for exploitation reaches its highest point.

This research demonstrates the cost to us all: somewhere in excess of £4.6 billion. But crucially, there is a cost in dislocation, disruption and a consequent failure to achieve the delivery of services and the saving of life.

Whilst measures have been put in place since the emergence of Covid-19 to avoid fraud and exploitation, there are clear lessons to be learnt and in due course, a thorough review of the nature and extent of attacks should take place. With a further range of substantial recovery measures announced by the Chancellor of the Exchequer on 8 July, more opportunity exists for those willing to defraud the nation as well as services and individuals, and further steps need to be taken urgently to coordinate across departments and agencies, concentrating on those areas where verification is most difficult to achieve and where self-certification opens opportunity for organised criminal behaviour. A recent exemplification of the challenge of tackling fraud is the example of the individual from Solihull who was arrested on suspicion of defrauding the furlough scheme of almost half a million pounds.

Policy Exchange's idea of an Economic Crime Forum, linked to the work of the National Cyber Security Centre and the National Crime Agency, is a useful proposal which could join expertise from a whole range of relevant services and businesses and avoid the danger of duplication, and 'reinventing the wheel'.

One early step which the Government could take is to ensure that in all areas where public funding or responsibility for delivery or procurement is involved, basic cyber security measures are authenticated, including through the supply chain. Identity assurance is not rocket science but requires the necessary expertise as well as awareness at policy level, to ensure that appropriate measures are not only put in place but tested on a regular basis.

It is clear, not just from the research undertaken for this publication, but from many recent high-profile incidents over identity theft, that lessons still need to be learnt and urgent steps to be taken in order to provide long-term assurance that security is given the priority it deserves.

The Rt Hon. the Lord Blunkett
Former Home Secretary (2001-5)

Executive Summary

COVID-19 Public Sector Disaster Fraud

- Research by Policy Exchange finds that fraud and error during the COVID-19 crisis will cost the UK Government in the region of £4.6 billion. The lower bound for the cost of fraud in this crisis is £1.3 billion and the upper bound is £7.9 billion, in light of total projected expenditure of £154.3 billion by the Government (excluding additional expenditure announced in the 8th July 2020 Economic Update).[1] The true value may be closer to the upper bound, due to the higher than usual levels of fraud that normally accompany disaster management.
- The UK Government response to COVID-19 is particularly vulnerable to fraud, owing to the novelty and speed with which new measures have been introduced and the size of the relief packages. Furthermore, the increased use of digital channels and third parties raises the opportunities for fraudsters to infiltrate the system.
- A range of actors, from individuals to public sector workers, corporations and organised crime networks have been shown to have participated in COVID-19 related fraud.

What is Public Sector Fraud?

- Fraud is an economic crime that is often associated with other crimes such as money laundering, bribery, corruption and collusion.
- Economic crimes encompass a range of activities that involve illegally gaining an advantage or inflicting a loss that involves money, finance or assets.[2]
- Public sector fraud is fraud where the government is the victim. This can include a range of behaviours, from individuals making fraudulent Universal Credit applications to opticians overcharging the NHS for services provided.
- The government has acknowledged that in 2017-18, between £2.8 billion and £22.6 billion was lost to fraud and error, outside the tax and welfare system.[3]

1. See Appendix 1 for more information regarding these estimates.
2. HM Government & UK Finance, Economic Crime Plan, 2019-22, July 2019, link
3. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

What is Disaster Fraud?

- Disaster fraud can be defined as a 'deliberate act to defraud individuals or governments after a catastrophe'.[4]
- Crisis management attracts fraudsters as it involves an outpouring of government aid, typically accompanied by low levels of due diligence.
- High levels of fraud have been recorded after a range of disasters, from Hurricane Katrina in the USA (2005), to Grenfell Tower in the UK (2017) and the recent Australian bushfires (2019-2020).

Fraud and the National Health Service

- The Department for Health & Social Care and the NHS are especially vulnerable to an increase in Mandate, Procurement, Recruitment and Payroll fraud as a result of the COVID-19 crisis.
- Even in normal times, the annual loss to the NHS from fraud is equivalent to the cost of employing an additional 50,000 fully qualified nurses, as pledged by the current Government in its Conservative Party manifesto.[5]

Cases of COVID-19 Public Sector Disaster Fraud

Fraud and the COVID-19 Economic Relief Schemes

- By leading the economic response to the COVID-19 crisis, HM Treasury and the Department for Business, Energy & Industrial Strategy are vulnerable to fraud.
- The speed with which Bounce Back Loans (BBL) are approved (82 per cent of loans approved compared to 50 per cent for CBILS) and the potential to make multiple applications pose a particular risk. Poor Companies House data has compounded the risk.
- The speed with which overstretched and underqualified councils have issued Business Support Grant Funds make these vulnerable to fraud. Bad practices such as sending cheques in the post have been reported to Policy Exchange.
- The Coronavirus Business Interruption Loan Scheme (CBILS) is one of the most secure against fraud, but this has hampered the effectiveness of the scheme, making BBLs necessary.
- The Coronavirus Job Retention Scheme is the most expensive and widely used support scheme and is also the most susceptible to fraud. Although HMRC have attempted to directly tackle fraud in this area, it is one of the most difficult schemes to monitor and HMRC had already received 1,868 claims of furlough fraud as of the end of May 2020.
- The approach taken for the Self-Employment Income Support Scheme, with HMRC only contacting those who are eligible, has minimised fraud, however there is a potential opportunity for individuals to exaggerate claims.

4. R. Brody & V. Kimball, 'Natural Catastrophe and Disaster Fraud', *Fraud Magazine*, December 2006, link
5. Fully qualified nurse on band 5 annual salary of £24,907.

- Benefit fraud has been a long standing issue, with the amount lost to fraud in 2019/20 equivalent to each benefit claimant gaining an additional £140 a year. Universal Credit in particular has been under scrutiny, as it has the highest rate of fraud at 7.6 per cent of expenditure and at 17 per cent of total payments. Changes to make Universal Credit more generous and more accessible to the public as a result of COVID-19, combined with the sharp increase in the number of applications, will increase the amount lost to fraud in this area.
- Public sector fraud is not a problem that is unique to the UK. Many other countries such as the USA, Australia, Canada, Germany, Italy and France have all suffered from COVID-19 related public sector fraud.
- Governments must learn from the experience of the COVID-19 crisis and increase the range of preventative measures and controls that need to be in place for disaster scenarios, so that they are better prepared for the next crisis.
- Widespread government awareness campaigns to alert the public sector to the possibility and risks of fraud and to enlist the assistance of the public to report fraud are key.
- Governments must investigate and prosecute COVID-19 crimes to maintain the confidence of the public. To do otherwise will risk threatening the sense of national unity and purpose that has emerged during the crisis.

The Impact of Fraud

- As with all crime, fraud has a range of costs. The first is the economic cost, which occurs directly as a result of the crime. The second is the psychological and physical cost, borne by victims and individuals subjected to the crime. The third is specific to public sector fraud and is the cost to society of trust in public sector organisations and institutions being eroded by the inability of the government to protect the public finances.

Economic Cost of Fraud

- Money lost to fraud has an opportunity cost, leaving fewer resources available for essential services such as the NHS, schools and law enforcement. Furthermore, pervasive fraud can prevent governments from offering services in the first place.
- The increase in detected public sector fraud since 2014 should be seen as a positive development, however it is important that going forward government department fraud rates are compared to their overall budgets to allow for accurate analysis. For example, it appears that the Department for Health and Social Care detected relatively high levels of fraud in 2018/19 (£7.8m) compared to the Department for Business, Energy & Industrial Strategy

(£3.6m). However, in light of the DHSC's significantly larger budget (£171bn vs. £7.5bn for BEIS), the DHSC actually has a relatively low detection rate.

- Fraud is notorious for being one of the most difficult crimes to gather accurate information on, which is largely due to persistent underreporting of fraud and issues relating to the recording of fraud. The Crime Survey for England and Wales revealed that in 2019, 36 per cent of incidents of crime experienced by respondents was fraud, but only 13 per cent of police recorded crime for the same period was fraud.[6]
- Some victims do not report fraud as they believe that it is not worth their time as they believe that it will not be investigated. Others are unwilling to report fraud because of the stigma of reporting it, given the level of co-operation that most acts of fraud require; this is similar to the stigma which exists around the reporting of rape.
- Fraud cases require difficult judgements to be made as to whether an overpayment was made as a result of fraud or whether the case is one of error. Different recording practices can therefore lead to inconsistent data.
- Civil servants in government departments may be wary of reporting fraud due to the negative media attention this can attract. Departments reporting zero fraud may not have the procedures in place to report and detect fraud.

Psychological and Physical Impact of Fraud

- Research has found that 45 per cent of fraud victims felt that the financial loss they experienced had an impact on their emotional wellbeing and 37 per cent reported significant psychological or emotional impact.[7]
- The reputational damage for some victims of being involved in a case of fraud can be severe, especially with regards to their employment prospects.
- Fraud in the NHS can have a direct impact on people's physical health, for example, faulty PPE leaving nurses vulnerable to contracting COVID-19.

Societal Impact of Fraud

- High levels of public sector fraud implies that the Government cannot be trusted to handle public sector finances. Fraud therefore erodes public trust in the Government and has the potential to create a crisis of confidence in the public sector.
- The erosion of trust in the Government has a range of negative consequences for society, including reducing participation in democracy and weakening compliance with the law.
- Fraud poses a national security risk as large-scale fraud damages the reputation of Britain as a safe and secure country, thereby reducing the willingness of our allies to cooperate and share

6. ONS, 'Crime Survey for England and Wales, year ending in December 2019', April 2020, Link
7. Police Foundation, 'More than just a number - improving the police response to fraud', 2018, link

information with us.
- Fraud impacts the integrity and reputation of the UK's financial services sector, which will play a vital role in the success of Britain after its withdrawal from the European Union (EU).

UK Government Counter Fraud Measures

- Responsibility for Government policy on *public sector fraud* rests in the Cabinet Office which is responsible for the counter fraud 'profession' and its function across the entirety of the public sector. Additionally, all major Government departments have dedicated units that investigate fraud related to their functions.
- Responsibility for investigating frauds against *individuals* and the *private sector* rests with the Home Office and myriad of investigative units in different law enforcement bodies (e.g. NCA, Regional and Organised Crime Units and individual police forces).
- The plethora of disparate fraud investigative units across Government and law enforcement means that there is little consistency or coherence in the overall effort to counter fraud. Accountability for outcomes is held by different Ministers with conflicting Ministerial priorities and objectives, resulting in a dilution of purpose, oversight, focus and accountability.
- The Government launched the counter fraud functional standard (GovS 013) in October 2018, to encourage the adoption of anti-fraud measures across Government organisations, however some of the standards do not go far enough.

Leadership and Criminal Investigation of COVID-19 Related Fraud

- Although the UK Government responded fast to COVID-19 related fraud, introducing a range of counter fraud and awareness raising preventative measures, a Minister for Fraud and Economic Crime should now be appointed to oversee the prevention, detection, investigation and prosecution of all COVID-19 related economic crimes against the public and private sector.
- The National Economic Crime Centre (NECC) should undertake a National Risk Assessment of COVID-19 economic crime and create a 'COVID-19 Economic Crime Hub' to coordinate the prevention, detection, investigation and prosecution of COVID-19 related fraud crimes committed against the UK Government.
- The NECC should also establish a COVID-19 Economic Crime Forum, bringing together all the agencies and Government investigative bodies dealing with COVID-19 related economic crimes, sharing best practice and looking to find synergies and overlaps between investigations.
- A single Fraud Hotline should be created for the public to report any aspect of fraud.
- HMRC and the Home Office / NCA should also lead a COVID-19

economic crime / fraud public awareness campaign encouraging the public to report crime related to COVID-19, specifically addressing the perception that fraud is victimless.

Using Technology to Prevent and Detect Public Sector Fraud

- Unless the UK Government makes use of the latest innovations in anti-fraud technologies, it is unlikely that it will be able to investigate fraud at the level and scale that the COVID-19 crisis requires. Furthermore, the crisis has exposed a number of long-term limitations to the public sector's digital anti-fraud infrastructure (particularly in relation to identity assurance and digital identity).
- The UK Government should deploy the latest anti-fraud technologies and data analytic techniques. It should also strengthen identity assurance and digital ID solutions across all government departments and take greater steps to detect and prevent fraudsters who are impersonating government departments and agencies.

Recommendations

Oversight, governance and accountability

- The Home Secretary and Chancellor of the Exchequer should revisit the recommendations in the Economic Crime Plan 2019-2022[8] and reconvene the Economic Crime Strategic Board[9] to agree a co-ordinated response to the monitoring, investigation and prosecution of COVID-19 economic crimes / frauds across government.
- The Prime Minister should create a new **Minister for Fraud and Economic Crime** (separate from the current portfolios of the Security Minister) to oversee the prevention, detection, investigation and prosecution of all fraud crimes, including COVID-19 related frauds. This Ministerial portfolio should straddle the Home Office and Cabinet Office.
- A **Minister for Fraud and Economic Crime** should make a strong public and political commitment to addressing all public sector fraud relating to the COVID-19 crisis, seek cross party consensus and announce how public sector COVID-19 related frauds will be monitored, investigated and prosecuted.
- The lead **Minister for Fraud and Economic Crime** should appoint a single law enforcement lead (Director General of the NECC) to be responsible and nationally accountable for the prevention, detection, investigation and prosecution of COVID-19 related economic crimes across the entirety of the private and public sector.
- The Home Office should provide substantial additional funding to resource a new Ministerial post for Fraud and Economic Crime and to significantly uplift the operational capability of the NECC within the National Crime Agency so that it can lead operationally for all types of COVID-19 fraud across the public and private sector.
- The National Economic Crime Centre (NECC) within the NCA should create a '**COVID-19 Fraud Crime Hub**' and **COVID-19 Fraud Crime Forum** to oversee and coordinate the prevention, detection, investigation and prosecution of COVID-19 related economic / fraud crimes across the entirety of the public sector of Government.
- The National Economic Crime Centre (NECC) should undertake a

8. HM Treasury & Home Office, 'Economic Crime Plan 2019-2022', July 2019, link
9. HM Treasury & Home Office, 'Economic Crime Strategic Board 2019 agenda and minutes', July 2019, link

National Risk Assessment of COVID-19 economic crimes / frauds.

- The Home Office / NCA should lead a COVID-19 fraud public awareness campaign encouraging the public to report crime related to COVID-19 - specifically addressing the perception that fraud is victimless.

Making COVID-19 fraud crime reporting easier

- The **Minister for Fraud and Economic Crime** should oversee a programme of work that examines how 'Action Fraud' and the National Financial Intelligence Bureau (NFIB) could be merged with the National Economic Crime Centre (NECC) at the NCA, leading to more effective reporting and monitoring of fraud allegations and the tasking of resources to investigate fraud.
- The Government should consider streamlining the reporting of COVID-19 economic crimes / fraud and launch a single **Fraud Hotline** for the public.
- A newly created '**COVID-19 Fraud Crime Hub**' should introduce common data standards across government for reporting of COVID-19 related fraud criminality.
- It is recommended that all Government departments reassure employees that there is strict confidentiality in the reporting of fraud.

Investigation and prosecution of COVID-19 fraud

- It is recommended that the NHSCFA conduct a review into NHS fraud during the COVID-19 crisis at the earliest opportunity in order to capture organisational learning and prevent fraud in the future.
- All COVID-19 related economic crimes / frauds should be monitored by the NECC and serious / organised COVID-19 related crimes tasked to teams of skilled investigators by NECC (e.g. City of London Fraud team, the SFO or Regional Organised Crime Units (ROCUs)).
- The CPS should be given additional resources to deal with the increased demands of prosecuting COVID-19 related fraud allegations.

In the event of another crisis:

- In the future, the government should make full transparency a condition of receiving state aid and of taking out government backed loans.

Using Technology To Prevent and Detect Public Sector Fraud

- To encourage the use of data analytics to tackle fraud:
  - The UK Government should explore the feasibility of creating a dedicated anti-fraud AI Lab to accelerate the adoption of AI to tackle fraud across the public sector.

- The 'COVID Fraud Hub' should be equipped with the latest innovations in anti-fraud technology (including document review technologies and AIs).
- The Department for Culture, Media and Sport (DCMS) should use its National Data Strategy to identify data assets across both the public and private sector that could support counter-fraud data analytics.
- The Government should look to increase private sector participation in the National Fraud Initiative to ensure that a greater range of private sector data is available to detect and fight fraud.
- The Counter Fraud Centre of Expertise should run a number of COVID-specific data sharing pilots in conjunction with HMRC and other departments.

- To improve identity assurance and verification across Government Departments, the follow measures should be adopted:
  - The Government should accelerate the creation of *Confirm My Identity* and provide clarity on the future of GOV.UK Verify.
  - Expand the scope and availability of the Government's Document Checking Service and increase private sector participation in the DCS pilot scheme.
  - Use Government data resources to improve identity proofing and verification processes.
  - Introduce rigorous identity checks for Companies House directors as part of the ongoing reform.
- To prevent fraudsters impersonating Government Departments and Agencies, Policy Exchange recommends that:
  - All banks accredited in the Coronavirus Business Interruption Loan Scheme and NHS Trust should be required to introduce the highest email authentication protocols to prevent domain spoofing.
  - The Government should further advertise the existence of the NCSC's Suspicious Email Service.

Introduction

Covid-19 - A global bonanza for fraudsters

The emergence of a digitalised interconnected world over the last two decades has radically affected crime patterns, shrinking opportunities for some criminals (through the use of CCTV, facial recognition and artificial intelligence) but providing new ones for many others, most notably in the areas of cyber and economic crime.

Prior to the COVID-19 crisis, a range of fraud and economic crimes were proliferating across nation state boundaries, but the pandemic has produced a once in a generation opportunity for fraudsters (whether individuals or organised crime groups) to pivot towards and exploit the new and almost unlimited crime potential that a global health crisis presents.

This is not an entirely new phenomenon. The rapidity with which governments have had to respond to the unprecedented challenges of disasters and crises creates opportunities for fraudsters to disguise themselves among the needy. Experts in disaster fraud describe catastrophic events as a:

> *"beacon for opportunistic predators and a magnet for various forms of deception for dishonest gain"*[10]

Fraudsters have now seized upon the opportunities that the COVID-19 crisis presents to mobilise and defraud individuals, businesses and governments across the world. Interpol issued a warning of 'financial fraud linked to COVID-19' advising the public that criminals are 'taking advantage of coronavirus anxiety to defraud victims online'.[11] It listed scams linked to the virus including telephone fraud and 'phishing emails claiming to be from national or global health authorities with the aim of tricking victims to provide personal credentials or payment details or to open an attachment containing malware'. On 19th March, the UK Medicines and Healthcare products Regulatory Agency reported on finding 2,000 online adverts related to coronavirus and seizing over 34,000 fake products, such as 'corona spray'.[12] The US Federal Trade Commission reported 27,862 complaints of COVID-19 related fraud between January 1st and May 17th 2020, with total fraud losses of $35.34m.[13]

At the private level, an increase in fraud has occured in part due to national lockdowns, which have forced hundreds of millions of people and businesses to conduct their lives online by turning to their laptops and

10. R. Brody & V. Kimball, 'Natural Catastrophe and Disaster Fraud', *Fraud Magazine*, December 2006, link
11. Interpol, 'INTERPOL warns of financial fraud linked to COVID-19', March 2020, link
12. Medicines and Healthcare products Regulatory Agency, 'Coronavirus: global crackdown sees a rise in unlicensed medical products related to COVID-19', *GOV.UK* [website], March 2020, link
13. Federal Trade Commission, 'COVID-19 consumer complaint data', 2020, link

smartphones as a way of maintaining interconnectivity with their friends and workplaces. This has increased the opportunities for fraudsters, as activities that would usually take place face to face have moved online. Businesses are also more vulnerable, as employees lack suitable IT infrastructure at home to fend off attacks.

Across the public sector, workplace pressure created in the midst of a fast moving crisis has meant that normal financial controls and due diligence have been loosened in the interests of saving lives, operational delivery and expediency, increasing the risk of large-scale fraud. This is not a new phenomenon, a fact highlighted in the Cabinet Office paper *Fraud in Emergency Management and Recovery - Principles for Effective Fraud Control*, released at the beginning of 2020:

> *"In emergency situations, policies, systems and processes have to be put in place rapidly. This limits the time that is available for reflection on what the criteria are for payments to be made or services to be delivered. It also limits the time for processes to be clearly defined, systematically recorded, and analysed.*
>
> *Inevitably, emergency payments have to be made quickly. This means the appetite for up-front controls to check eligibility for a payment (which may delay those payments) is low…*
>
> *As a result of the above factors, the threat and risk of vulnerabilities to fraud are inherently much higher in emergency management."*[14]

A number of government departments have been affected by COVID-19 public sector fraud, not least the Department of Health and Social Care, Her Majesty's Revenue and Customs and Department for Work and Pensions, a problem that has been compounded by fraud specialists within Government departments being diverted from tackling fraud to delivering essential services.

The variety in the nature of different types of frauds and other economic crimes instigated poses an additional challenge to all governments, whose focus has naturally been on saving lives and the economic well being of their nations. An unpleasant trade-off has emerged, where governments have had to balance the need to design relief packages that are accessible to those in need without giving handouts to criminals and balance the necessity for speed in the delivery of goods such as PPE without sacrificing the due diligence that ensures transactions are occurring with legitimate suppliers.

Faced with this increase in fraud as a result of COVID-19, how should nation states respond? Governments must ensure that the risks posed by fraud, to the Treasury and public finances, to health and to society as a whole are not neglected in the response to this crisis.

In the past, a good deal of fraud has been viewed by some as an unintended consequence of an increasingly digitised and global e-commerce and financial sector, a victimless crime and a crime that is too complex to investigate. The scale of COVID-19 fraud is, however,

14. International Public Sector Fraud Forum, 'Fraud in Emergency Management and Recovery: Principles for Effective Fraud Control', February 2020, link

unprecedented, global, and requires a co-ordinated investigative response or countries will face a public backlash of anger from their populations who will rightly feel that their taxes have been mishandled.

Detecting and preventing fraud is a key element of sound public finances and should therefore be a priority for this Government. It is not reasonable to expect the public to hand over a share of their personal finances month after month if the government cannot be trusted to responsibly manage this money. Considering the pressure that will emerge after the COVID-19 crisis to cut costs, reducing fraud will be one of the most equitable and achievable options available and will be vital to the government's ability to achieve other objectives, such as levelling up the North.

This paper focuses in particular on public sector fraud. It explores what the investigative response has been to date, what it should be going forward and the likely implications of a lack of action by law enforcement agencies.

Arguably, the UK is a world leader in many aspects of countering public sector fraud, not least prevention and policy, but long standing deficiencies in the investigation and prosecution of fraud need to be rectified if public confidence in the nation's ability to detect and combat public sector fraud is to be retained.

1. What is Fraud?

An Introduction to Fraud and Disaster Fraud

Fraud is an economic crime that is often associated with other crimes such as money laundering, bribery, corruption and collusion. Economic crimes encompass a range of activities that involve illegally gaining an advantage or inflicting a loss that involves money, finance or assets.[15] Fraud is essentially a form of theft, involving dishonesty.

UK Definition of Fraud

In 2014, the government created the following definition of fraud based on that set out in the Fraud Act 2006:

> *"The making of a false representation or failing to disclose relevant information, or the abuse of position, in order to make a financial gain or misappropriate assets".*[16]

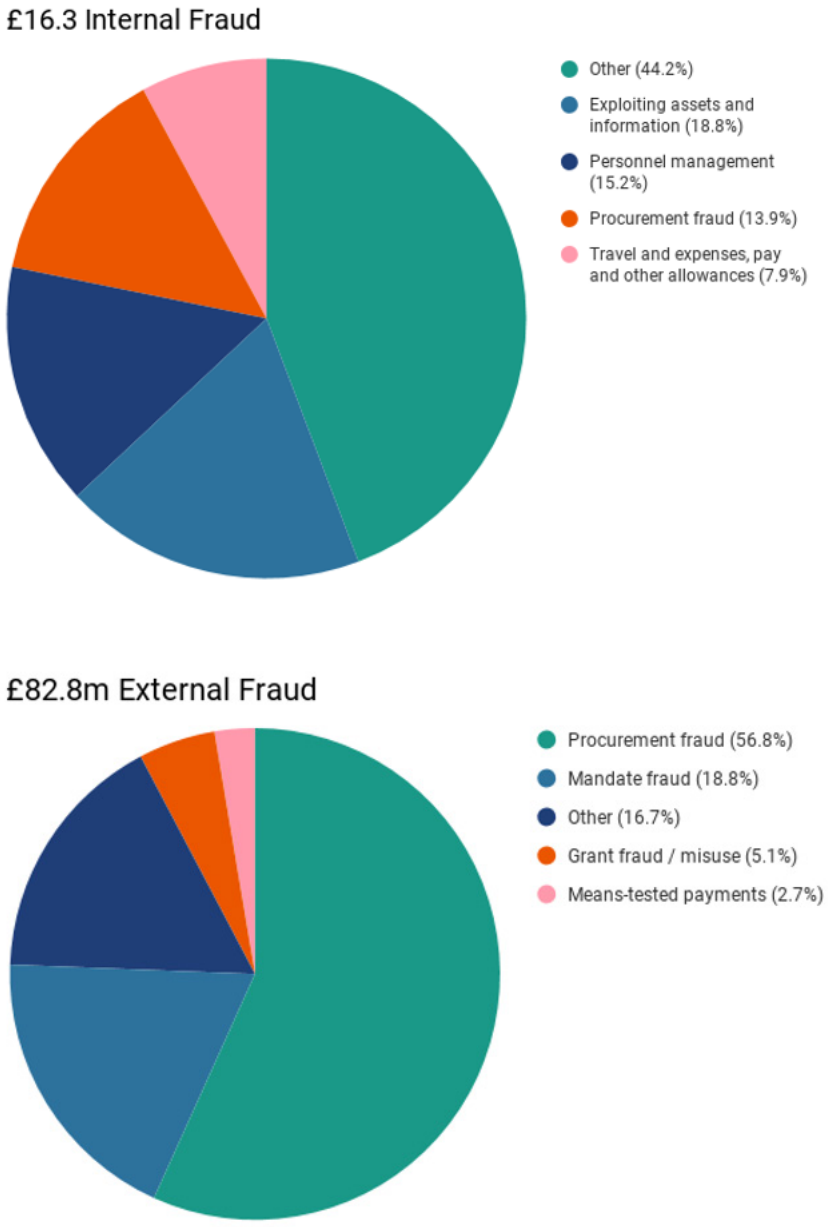
Public Sector Fraud

Public Sector fraud refers to fraud where the government is the target and victim. As there are a wide range of behaviours that fall under the definition of fraud, public sector fraud can be further broken down into internal and external fraud. Internal fraud is fraud committed by public sector workers such as civil servants, whereas external fraud is committed by suppliers, contractors and the public.[17]

An example of internal fraud from 2019 includes the case of the DWP civil servant who defrauded the government of over £40,000, by using other claimants' National Insurance numbers to pay benefits into bank accounts she controlled.[18] Another case involved a civil servant at the Department for Education, who stole £1 million over two years by siphoning leftover funds into shell companies. Worryingly, had it not been for his mother who reported him, it is unlikely that the Department for Education would have discovered this fraud.[19] Figures 1 and 2 show the breakdown of internal and external fraud committed against the government in 2018-19. In this period 16 per cent of fraud detected by government departments was internal fraud (£16.3m), and 84 per cent was external fraud (£82.8m).[20]

15. HM Government & UK Finance, 'Economic Crime Plan, 2019-22', July 2019, link
16. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link
17. National Audit Office, 'Cross-government Fraud landscape review', 2016, link
18. BBC, "Corrupt' civil servant jailed for universal credit fraud', February 2019. Link
19. Sophie Jamieson, 'Civil servant stole £1m from Government to buy a luxury flat', *The Telegraph*, June 2016, Link
20. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

Figure 1 and 2: Internal and external detected fraud broken down by typology for all government departments and their arm's-length bodies, 2018-19.[21]



Cybercrime and fraud

The Crown Prosecution Service provides the following definition of the two types of activity that constitute cybercrime:

Cyber-dependent crimes - crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).

21. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)."[22]

According to the Crown Prosecution Service, cyber-enabled fraud is one of the most common cybercrime offences.[23] Most external fraud would fall under the category of economic related cyber-enabled crime, due to the fact that by moving the provision of Government services online, criminals seeking to target these services must do so online too. Nevertheless, some fraudulent activities can be classified as cyber-dependent crime, particularly in cases of internal fraud, where public sector employees use 'privileged access to computers and networks' to commit fraud.[24]

Disaster Fraud

The amount of fraud that occurs in different countries at different times depends on circumstance and the respective opportunities available. Disasters and crises are well known as a magnet for fraud. In fact the links between economic crime / fraud and the emergency management of disasters or crises are well understood internationally with a body of literature highlighting the opportunities that emergencies present to fraudsters.

Disaster fraud has in fact become a specialist research area and is defined as:

> *"A deliberate act to defraud individuals or governments after a catastrophe and can be divided into five primary categories: charitable solicitations, contractor and vendor fraud, price gouging, property insurance fraud, and forgery"*[25]

Fraudsters are attracted to crisis management, as these situations ordinarily involve an outpouring of government aid, typically accompanied by low levels of due diligence as a result of a necessity to ensure that finance reaches recipients quickly.

An example of this in the UK occured after the Grenfell Tower disaster. The government rightly stepped in after the tragedy of Grenfell Tower offering residents emergency accommodation, a minimum £5,500 payment from the Grenfell Tower Residents' Discretionary Fund and new housing. However, as with all generous government schemes, some saw this as an opportunity to commit fraud. Alvin Thomson defrauded the state of emergency accommodation costing £90,000 by claiming to be a squatter in the tower[26], while others defrauded the government of hundreds of thousands of pounds by claiming to be sharing flats with residents who did not survive. A finance manager at Kensington and Chelsea Council was also found to have taken £62,000 from the Grenfell Tower Fund.[27]

A more recent international example is fraudulent claims for bushfire relief assistance linked to the Australian bush fires in 2019-2020. The Australian Red Cross reported receiving 'computer-generated applications for bushfire relief assistance', which can result in grants up to $20,000.[28]

22. The Crown Prosecution Service, 'Cybercrime - prosecution guidance' [website], link, (accessed June 2020).
23. The Crown Prosecution Service, 'Cybercrime - prosecution guidance' [website], link, (accessed June 2020).
24. The Crown Prosecution Service, 'Cybercrime - prosecution guidance' [website], link, (accessed June 2020).
25. Fraud Magazine, 'Natural catastrophe and disaster fraud - Calamity criminals', 2006, link
26. BBC News, 'Grenfell - Man who claimed to be squatter jailed', November 2019, link
27. Sky News, 'The fraudsters who took advantage of Grenfell', November 2019, Link
28. The Sydney Morning Herald, 'Cyber thieves target charity bushfire grants', 2020, link

One of the most infamous examples of disaster fraud is Hurricane Katrina, when billions of dollars in federal disaster relief poured into the Gulf Coast region leading to unprecedented levels of fraudulent claims:

> *"The U.S. Congress originally set aside $62 billion for reconstruction, but the amount was eventually increased to more that $110 billion…Normal federal contracting rules had been suspended in the rush to help the displaced and re-open New Orleans. The sheer speed in which contracts were handed out was unprecedented. Hurricane Katrina relief money disappeared at a rate of more than $500 million a day. More than 80 per cent of the $1.5 billion in contracts was awarded without bidding[29]".*

The Hurricane Katrina Fraud Task Force (established in September 2005) subsequently investigated 17,000 complaints and brought federal charges against 907 individuals in 43 federal judicial districts across the country between 2005-8[30]. The US Government subsequently acknowledged that the response to Katrina Fraud had not been adequate and created the National Center for Disaster Fraud (NCDF)[31] in 2005 to address this challenge in future disasters:

> *"The NCDF is a national coordinating agency within the Department of Justice's criminal Division dedicated to improving the detection, prevention, investigation and prosecution of criminal conduct related to natural and man-made disasters and other emergencies, such as coronavirus (COVID-19)"*

The creation of the NCDF now puts the USA in a better position to deal with the onslaught of fraud that is occurring in the COVID-19 crisis.

29. Fraud Magazine, 'Natural catastrophe and disaster fraud - Calamity criminals', 2006, link
30. Government Technology (gt), 'Hurricane Katrina Fraud Task Force Brings Storm of Justice', 2008, link
31. The United States Department of Justice, National Centre for Disaster Fraud, accessed May 2020, link

2. COVID-19 Public Sector Disaster Fraud

Why COVID-19 poses a particular opportunity for fraudsters

There are a number of elements of the COVID-19 crisis that make the Government response particularly vulnerable to fraud. The first is the novelty and speed with which new measures have had to be introduced. Businesses had just days to prepare for emergency ('lockdown') measures and enforced social distancing, so the Government had to rapidly design and roll out new assistance schemes in order to prevent financial distress. The speed with which the Government made aid available to businesses and individuals provided opportunities for fraudsters to take advantage of the situation. The sheer size of the Government relief package also acted as a magnet for fraudsters.

Furthermore, in the 2016 National Audit Office *Cross-government Fraud landscape review*, it was specifically highlighted that 'greater use of third parties and digital channels' increases the risk of fraud.[32] The UK Government's strategy for dealing with the COVID-19 crisis has accelerated these trends, as enforced social distancing has increased the number of interactions handled online and led to organisations such as the NHS having to rely on new third party intermediaries for the provision of goods such as PPE. These risks are compounded by the fact that there is no single identifiable threat. A small selection of profiteering individuals, corporations and organised crime networks are seeking to defraud the system through a range of mechanisms.

The Government has highlighted two types of fraud that it believes will pose the greatest threat to the public sector over the course of this crisis:

- First party application fraud (where an applicant for a government support scheme misrepresents their circumstances to become eligible e.g. when applying for Universal Credit).
- Third party impersonation fraud (where a third party impersonates an individual or business to gain access to government financing options e.g. by impersonating a business and applying for Business Support Grants). [33]

Four UK Government departments have been particularly susceptible to

32. National Audit Office, 'Cross-government Fraud landscape review', 2016, link

33. Government Counter Fraud Function, 'Fraud Control in Emergency Management: COVID-19 UK Government Guidance', Link

fraud as a result of the COVID-19 crisis. The first is the Department for Health & Social Care and the NHS, which has had to rapidly shift and expand its operations to deal with the unique challenges of the COVID-19 crisis. Additionally, Her Majesty's Revenue and Customs, the Department for Work and Pensions and the Department for Business, Energy & Industrial Strategy have all been vulnerable to fraud after instituting a range of measures to protect the UK economy whilst emergency restrictions in public life were invoked.

Research by Policy Exchange finds that fraud and error during the COVID-19 crisis will cost the UK Government around £4.6 billion. The lower bound for the cost of fraud in this crisis is £1.3 billion and the upper bound is £7.9 billion, of total projected expenditure of £154.3 billion by the Government (excluding additional expenditure announced in the 8th July 2020 Economic Update).[34] This range has been calculated by using a combination of expected fraud rates for different types of Government expenditure created by the Cabinet Office and the Department for Work and Pensions. The true value may be closer to the upper bound, due to the higher than usual levels of fraud that accompany disaster management. This is a serious squandering of public finances and properly resourced post event assurance will be required to reassure the public that every possible step has been taken to reduce this level of fraud.

Fraud and the National Health Service (NHS)

The COVID-19 crisis has been particularly challenging for the NHS, which has had to rapidly redeploy its operations to tackle COVID-19. Amidst the backdrop of disruptions to global supply chains and a surge in demand for ventilators and PPE, the NHS has had to contend with serious supply and staff shortages, which fraudsters have been keen to take advantage of. Even in normal times, the vast expenditure of the NHS makes it a target for economic criminals.

The NHS Counter Fraud Authority (NHSCFA), sponsored by the Department of Health and Social Care Anti-Fraud Unit, was established in 2017 to tackle NHS fraud, bribery and corruption (where the NHS is the victim). In their annual Strategic Intelligence Assessment, the NHSCFA produces an estimate of the cost of fraud to the NHS, as well as intelligence regarding the characteristics of emerging fraud threats. It has identified 123 different types of fraud committed against the NHS (by employees, patients, suppliers or third parties), which costs the NHS £1.27 billion annually (Figure 3). This is a sum equivalent to employing an additional 50,000 fully qualified nurses (pledged by the current Government in its Conservative Party manifesto).[35]

34. See Appendix 1 for more information regarding these estimates.

35. Fully qualified nurse on band 5 annual salary of £24,907.

Figure 3: Annual cost of NHS Fraud, broken down into 13 Thematic Fraud Areas. [36]

NHS Procurement

NHS procurement refers to the process by which the NHS purchases goods (e.g. equipment and medicines) and services (e.g. GP services) from both public and private sector sources. In 2018/19, the Department for Health and Social Care gross procurement budget was approximately £70bn, of which around £18.2 billion was spent on medicine and £6 billion was spent on hospital consumables (e.g. syringes and gloves).[37] Responsibility for NHS procurement is split between the Department for Health and Social Care, NHS England and Public Health England.[38]

There are four key existing types of fraud, which have been identified as likely to become more problematic as a result of COVID-19. These are: mandate fraud; procurement fraud; NHS recruitment fraud and payroll fraud:

- **Mandate fraud** occurs when an individual impersonates a third party individual or organisation that regularly supplies goods or services to the NHS, and urgently requests payment to be made to a new (their own) bank account. Criminals obtain supplier details through a variety of means, ranging from '*corrupt staff, publicly announced contracts and online logs of supplier contracts*'.[39] This poses a particular threat in this crisis, as the urgent nature of such requests (a technique used to pressure staff into complying without due diligence) appears more valid. In particular, a tightening of the requirements to pay suppliers within 7 days, instead of the usual 30 days combined with the lack of training of new staff recruited as a result of COVID-19 increases the opportunity for mandate fraud to occur.
- **Procurement fraud** relates to '*collusion, bribery and corruption within the pre-tender stages of the procurement and commissioning process*'.[40] Fraud in the pre-tender stage of procurement can involve behaviours such as suppliers engaging in price-fixing.[41] Given the rapid onset of the COVID-19 crisis and urgent necessity for supplies in the face of unprecedented global demand, the Government has, since March 2020, relaxed the rules concerning NHS procurement to increase the ability of the NHS to rapidly procure the necessary goods and services to tackle COVID-19.[42] This includes the procurement of PPE (with up to 5 different pieces required to treat COVID-19 patients and a single trust requiring 72,000 items of PPE a day, the Government has already spent £15 billion on PPE[43]), ventilators and private sector beds. The fact that face-to-face meetings with suppliers are no longer possible has increased the risk of procurement fraud. With the UK described as a '*procurement fraud*

36. NHS Counter Fraud Authority, 'NHS Fraud Reference Guide', May 2020, link
37. NHS Digital, 'Prescribing Costs in Hospitals and the Community, England 2017/18', November 2018, Link; Department of Health and Social Care, 'The NHS Long Term Plan', 2019, Link
38. Institute for Government, 'Explainers: NHS procurement', 2020, Link
39. NHS Counter Fraud Authority, 'Mandate fraud risks', accessed May 2020, link
40. NHS Counter Fraud Authority, 'Procurement & commissioning fraud', accessed May 2020, link
41. National Fraud Authority, 'Procurement Fraud in the Public Sector', October 2011, Link
42. Cabinet Office, 'Procurement Policy Note - Responding to COVID-19', 2020, Link
43. F. Islam, 'Why a billion items of PPE is not enough', BBC, April 2020, Link; HM Treasury, 'A Plan for Jobs 2020', *GOV.UK* [website], July 2020, link.

capital' in 2019, the NHS is particularly vulnerable in this area.[44]

- **NHS Recruitment** is another area where the Government has been forced to relax regulations in order to increase the flexibility of the NHS to respond to the COVID-19 crisis. For example, in urgent cases employers may now accept scanned copies of documentary evidence and photographs of identity. NHSCFA has therefore raised concerns that a minority of new recruits may provide false identity documents, or falsely claim to have certain experience or qualifications.[45]
- **Payroll Fraud.** The highly irregular circumstances under which NHS staff have now had to operate has also increased the risk of payroll fraud, which occurs when there are fraudulent claims concerning the hours worked by staff. This can include exaggerated claims for hours worked and expenses, multiple salary entries and remaining on the payroll system post COVID-19. The issue of payroll fraud is exacerbated by the crisis, as the quantity and complexity of payrolls to be authorised has increased significantly.

Although fraud is often committed by individuals seeking a quick profit, it is worth noting that those who will be targeting the NHS are often part of sophisticated Organised Crime Groups (OCGs). For instance, the German government almost lost €2.4m to fraudsters who tried to sell them 10 million masks that did not exist.[46] The payment was eventually blocked (€500,000 of which was already en route to Nigeria), but the complex nature of the scam, which involved fake companies and websites in Spain, Ireland and the Netherlands, highlights the scale of the threat that is being faced.

It is also noteworthy that a national exercise on the prevention of procurement fraud in the NHS was initiated in 2019 with the next phase due to start in May 2020. This phase involves collecting data from providers but has been postponed due to the COVID-19 health crisis.[47] Whilst understandable in light of the immense pressure that the NHS is facing, the collection of data concerning fraud is critical to understanding and combating one of the most opaque yet prevalent crimes that exists. It is recommended therefore, that the NHSCFA conduct a review into NHS fraud during the COVID-19 crisis at the earliest opportunity in order to capture organisational learning and prevent fraud in the future.

44. Supply Management, Allen, A.,'UK a 'procurement fraud capital', 2019, Link
45. NHS Counter Fraud Authority, 'NHS recruitment fraud risks'. May 2020, link.
46. The Economist, 'The pandemic is creating fresh opportunities for organised crime', May 2020, Link
47. NHS Counter Fraud Authority, 'National exercise on procurement fraud on hold due to COVID-19', May 2020, Link

Fraud and COVID-19 Economic Support Schemes

The Government has had to rapidly introduce a range of measures to help businesses overcome the crippling effects of lockdown and social distancing and in order to protect the UK economy. Government support includes: Coronavirus Job Retention Scheme; coronavirus Statutory Sick Pay Rebate Scheme; deferral of VAT payments; deferral of Self-Assessment payments; Business Rates relief for the retail, hospitality and leisure industry and nurseries; coronavirus Small Business Grant Fund; Coronavirus Retail, Hospitality and Leisure Grant Fund; Cultural Recovery Fund; Self-Employment Income Support Scheme; coronavirus Business Interruption Loan Scheme; coronavirus Future Fund; coronavirus Bounce Back Loan; coronavirus Large Business Interruption Loan Scheme; COVID-19 Corporate Financing Facility; as well as introducing changes to make Universal Credit (UC) more accessible.[48] A summary of the fraud risks for some of these schemes are provided below.

The Chancellor, Rishi Sunak, began announcing these measures on 17th March 2020 and faced with the rapid onset of the crisis, officials at the Treasury had just days to create schemes that would have usually been designed over months and years.

Further Government support was announced by the Chancellor, Rishi Sunak in his Economic Update on the 8th July 2020, in the form of a Job Retention Bonus; Kickstart Scheme; a boost to worksearch, skills and apprenticeships; reduced VAT for hospitality, accomodation and attractions; Eat Out to Help Out; Infrastructure package; public sector and social housing de-carbonisation; Green Homes Grant and a Stamp Duty Land Tax temporary cut.[49] The Chancellor acknowledged the risk that fraud poses in this debate, highlighting that corruption and fraud 'costs billions, if not tens of billions, of pounds; that is money lost to the Exchequer that we can use to fund public services, and it also means that our local authorities in particular do not get the quality of services that they need to provide for their residents.'[50]

Although some of these schemes are vulnerable to fraud, such as the Eat Out to Help Out scheme (for instance, by food service establishments creating receipts for meals not served), sufficient information on the delivery of these schemes was not available when this report came to be printed to allow for a more detailed analysis of the specific fraud risks. We have therefore not included losses as a result of the defrauding of these schemes to the estimate in this paper of the amount that will be lost to fraud over the course of this crisis.

A few commentators warned of the criminal side effects of introducing these measures from the outset:

> *"There will be fraud, and a black market, and loopholes to be exploited on a massive scale"*[51]

Whilst the Chancellor and HM Treasury were fully aware of the potential

48. GOV.UK, 'Financial support for business during coronavirus (COVID-19), May 2020, Link
49. HM Treasury, 'A Plan for Jobs 2020', *GOV.UK* [website], July 2020, link.
50. R. Sunak, 'Economic Update', *Hansard* [website], July 2020, link.
51. M. Lynn, 'Rishi Sunak's wartime economy', *The Spectator*, March 2020, link

for fraud from these schemes, there appeared to be little that could be done other than attempt to 'fraud proof' them by design from the outset. There was a clear trade off between making these schemes less bureaucratic and complex on the one hand and less susceptible to fraud on the other. The true costs of these schemes, including the inevitable default on a large share of the loans, is as yet unknown.

Considering the scale of the economic relief packages, preventing and detecting fraud across the various schemes is an immense task that the Government is not equipped for. It would have been beneficial to have uncovered some of the secrecy surrounding fraudulent claims by increasing the transparency of the COVID-19 economic support schemes. In the future, the government should make full transparency a condition of receiving state aid and of taking out government backed loans. Firstly, this would act as a deterrent to some fraudsters, who may fear additional scrutiny and would not want a public record of their involvement in such schemes. Secondly, this would aid in the detection of fraud committed by corporations, as employees and directors could access the records of exactly what was being claimed. They could also more easily determine themselves whether anyone was impersonating their company.

Bounce Back Loan Scheme (BBLS)

As of the 2nd June 2020, £31 billion had been lent out under the government COVID-19 schemes, but of this over two thirds has been lent out through the Bounce Back Loan scheme, which is also the scheme most vulnerable to fraud.[52] As of the 5th July 2020, £31 billion had been lent out under the BBLS alone, which has the highest share of applications approved of all the loan schemes, at 82 per cent.

52. Robertson, H. 'UK coronavirus loans top £31bn but just half of CBILs approved'. City A.M., June 2020, Link

Bounce Back Loan Scheme (BBLS)[53]

- Available from 4th May 2020.
- Created to increase the speed with which small businesses (intended for companies who employ less than 10 people and the UK's 900,000 sole traders) could access finance.[54]
- UK based businesses, established before 1 March 2020, negatively affected by coronavirus are eligible for BBLS. Businesses must not have been classed as a 'business in difficulty' on 31 December 2019.
- Eligible firms can borrow between £2,000 and up to 25 per cent of turnover, with a maximum loan of £50,000 for 6 years.
- No fees or interest payable for the first 12 months.
- Loan 100 per cent guaranteed by the government.
- 11 lenders are participating in the scheme (AIB, Bank of Ireland UK, Bank of Scotland, Barclays, Clydesdale Bank, Danske Bank, HSBC UK, Lloyds Banks, NatWest, Santander, Skipton Business Finance, Starling Bank, The co-operative bank, RBS, tide, TSB, Ulster Bank, Yorkshire Bank). If rejected by one lender, can still apply to other lenders.
- Application process involves a short online application form (requires information such as annual turnover) and a self-declaration of eligibility.

The key factor that makes the BBLS more vulnerable to fraud is the emphasis on speed. BBLS should reach applicants within days, but in order to achieve this the government requires banks to drop the majority of due diligence checks on borrower viability in return for which the government guarantees 100 per cent of the loan. More than 69,000 BBLs totalling more than £2 billion were approved in the first 24 hours of the scheme being made available.[55]

Many banks have raised concerns about the risk of fraud with these loans. NatWest has reviewed around 20 per cent of applications that were flagged as potentially fraudulent.[56] One particular issue is the fact that companies are able to make applications to multiple banks under the scheme, thereby exceeding the £50,000 limit per applicant. Another is the lack of an identity check in the British company registration service. Once a company is registered with Companies House, even if a company is registered in somebody else's name, it is still possible to generate data flows, link the company to data from HMRC and make the company look legitimate. It is suspected that some fraudsters spend years creating fake company profiles in order either to sell them or to commit fraud. These companies are the kind that would be able to gain access to BBLs. Furthermore, standard practice to prevent multiple applications would be to register a floating charge in Companies House, but this can take days to execute. Considering the 24 hour turnaround of some BBLS, this leaves a window of opportunity for fraudsters to take out multiple loans. Furthermore, Companies House data is notoriously unreliable, with some

53. GOV.UK, 'Apply for a coronavirus Bounce Back Loan', May 2020, **Link**
54. Bounds, A. & Barrett, C. 'How will the UK's 'bounce back' loans work?', Financial Times, 2020, Link.
55. HM Treasury, 'Over 69,000 loans approved in the first day of the Bounce Back Loan Scheme', May 2020, Link
56. Lucy Burton, 'Banks fear action by watchdog after doling out emergency loans', The Telegraph, May 2020, Link

individuals using different addresses and middle names to run multiple companies. One senior bank executive has complained that

> *"Fraud risk is huge because there is currently no effective way of preventing multiple applications, and the speed required means the simplified application process might not allow for normal checks on ID,"* [57]

UK banks have warned that they expect between 40 and 50 per cent of BBLS to default. In light of the lack of personal guarantees, this could leave the government having to guarantee up to £9.25 billion (in light of the £18.5 billion lent under the scheme). The fact that the average loan is approximately £30,000 complicates the issue, as banks and the Government will be reluctant to drag small and family run businesses through the courts over such small sums of money. This has been described by executives as 'logistically impossible and a "PR disaster"'.[58]

Although HMRC has announced that it will be performing retrospective checks on BBLS, especially for those that default, this will not be possible if such a large share of loans default. Improved data and practices by Companies House would have played a key role in minimising risk in this area. Although the UK *Economic Crime Plan, 2019-22*, has highlighted that Companies House is being reformed, with changes including developing new technological solutions to check the verity of information received, increased data sharing to verify ownership information and increased cooperation with law enforcement, the process has been described as 'ongoing', and it is unclear when this is set to be complete.[59] In light of the vulnerabilities this crisis has exposed, the Government and BEIS should expedite reform of Companies House.

In the meantime, the Government should capitalise on findings from the Behavioural Insights Team and include information regarding the maximum fine and prison sentence for attempting to defraud the government, alongside the honesty statement included on the application form. This includes:

- Conspiracy to defraud: Maximum 10 years' custody.
- Fraud Act 2006 (section 1) Maximum 10 years' custody.
- Cheat the public revenue: Maximum Life imprisonment.[60]

57. D. Thomas, S. Morris & N. Megaw, 'Bankers win assurances on rules for UK bounce back loans', Financial Times, April 2020, Link
58. S. Morris, G. Parker & D. Thomas, 'UK banks warn 40%-50% of 'bounce back' borrowers will default', Financial Times, May 2020, link
59. HM Government & UK Finance, Economic Crime Plan, 2019-22, July 2019, link
60. JMW, 'The Growing Spectre of Furlough Fraud', May 2020, Link

Business Support Grant Funds

Small Business Grants Fund (SBGF) scheme[61]

- £10,000 one-off taxable cash grant for small businesses in England that occupies property, but pays minimal or no business rates.
- Businesses must be eligible for small business rate relief or rural rate relief on 11 March 2020.
- Eligible businesses can obtain multiple grants for multiple properties, but these cannot include parking spaces / car parks or properties used for personal use e.g. moorings.
- This grant counts towards the total de minimis state aid that businesses are permitted over a 3 year period.
- Applicants must declare to their local council that they will not exceed the state aid temporary framework threshold of €800,000 and that they were not an 'undertaking in difficulty' on 31 December 2019.
- Although local council's usually contact eligible businesses with details of how to claim, those who have not been contacted but believe they are eligible can still contact their council to try and claim.

Retail, Hospitality and Leisure Business Grants Fund (RHLGF)[62]

- One-off taxable cash grant for businesses in England in the retail, hospitality or leisure sector with a rateable value of less than £51,000 on 11 March 2020.
- Includes properties being used as for example a shop, restaurant, pub, cinema, estate agent, gym or hotel.
- £10,000 grant for businesses with a property that has a rateable value of £15,000 or under and £25,000 grant for businesses with a property that has a rateable value of more than £15,000 but less than £51,000.
- Eligible businesses can obtain multiple grants for multiple properties, but these cannot include parking spaces / car parks or properties used for personal use e.g. moorings.
- This grant counts as state aid under the COVID-19 Temporary Framework.
- Applicants must declare to their local council that they will not exceed the state aid temporary framework threshold of €800,000 and that they were not an 'undertaking in difficulty' on 31 December 2019.
- Although local council's usually contact eligible businesses with details of how to claim, those who have not been contacted but believe they are eligible can still contact their council to try and claim.

Local Authority Discretionary Grants Fund[63]

- Grants for small and micro businesses not covered by SBGF and RHLGF.
- Grants of £25,000, £10,000 or any amount under £10,000.
- Eligible businesses will be based in England, have relatively high and ongoing fixed property-related costs for a property with a rateable value or annual mortgage/rent payments below £51,000 on 11 March 2020.
- Businesses must also demonstrate that their income has fallen as a result of coronavirus.
- Local councils have been asked to prioritise businesses such as market traders or small businesses using flexible workspaces. Nevertheless, each local council has discretion as to how to distribute funding.
- Grants from this fund count towards state aid.

61. Check if you're eligible for the coronavirus Small Business Grant Fund, *GOV.UK* [website], (accessed June 2020), link.

62. Check if you're eligible for the coronavirus Retail, Hospitality and Leisure Grant Fund, *GOV.UK* [website], link, (accessed June 2020).

63. Apply for the coronavirus Local Authority Discretionary Grants Fund, *GOV.UK* [website], link, (accessed June 2020).

As of the 28th June 2020, £10.5 billion has been provided to over 861,000 business premises through the Small Business Grant Fund and the Retail, Hospitality and Leisure Grant Fund.[64] Fraudsters are using a range of techniques in order to attempt to illegally obtain business grants. These include impersonating a legitimate business or using a fake company that has already been established. Claims have also been made for properties that are no longer in use. Policy Exchange has received reports of six fraudulent business grant applications being made on behalf of a single high street bakery chain, which was only discovered when local councils attempting to make payments found that the bank accounts provided had been frozen. It was particularly alarming that the fraudsters had the business rates account numbers of the outlets they were trying to impersonate, which means that they had managed to obtain sensitive information, or that an internal employee was involved in the crime.

Although all those overseeing the distribution of COVID-19 economic relief packages should have taken steps to minimise the ability of fraudsters to take advantage of these schemes, local authorities who are responsible for grant funding have limited counter fraud capabilities and have not been incentivised to improve these. Furthermore, the significant increase in the scale of operations that local councils have had to undertake has meant that untrained business rates officers are working on and giving out grants, which increases the risk that fraudulent applications will not be recognised. Evidence has emerged that local councils are failing to carry out the appropriate security checks to ensure that grant fund money is reaching legitimate businesses. One local authority who carried out checks discovered that one in ten applications for business grants were potentially fraudulent.[65] Most councils are relying on data from Companies House, which as highlighted above, is not a reliable source of information.

Nick Downing, Chief Intelligence Officer at Cifas, a fraud prevention organisation, has warned that the enormous pressure on local councils to ensure that businesses receive funds quickly has led to councils approving grants without the appropriate due diligence procedures, such as checking that a firm is even legitimate. He believes that at least £100 million could be taken fraudulently, and that the chance of recovering this money is minimal.[66]

With councils being judged in the media for the speed with which applications are processed and for the total size of payouts, it is evident that the key performance indicators are set to incentivise fraud. Policy Exchange has received reports of some councils sending out cheques to businesses to expedite the process and therefore make claims about the success of their operational efficiency. This means that fraudsters do not even need to provide a business bank account to receive payment, and local councils do not even have available to them information such as the bank account numbers of whom they have been sending money to. They would have to go to the bank and request information regarding the accounts that payments were made for every individual cheque in order

64. HM Treasury, 'A Plan for Jobs 2020', GOV.UK [website], July 2020, link.

65. M. Hunt, 'Opportunistic fraudsters could steal £100m of Government's coronavirus emergency funding', *The Telegraph*, 18 April 2020, link

66. M. Hunt, 'Opportunistic fraudsters could steal £100m of Government's coronavirus emergency funding', *The Telegraph*, 18 April 2020, link

to conduct post event assurance. Although the Government has stated that it is providing advice on how councils can minimise fraud pre- and post-payment, it should have advised councils against such practices from the outset.[67] Furthermore, councils are reporting that the support offered from the government, in the form of the software Spotlight, has not been useful.

It is also worth noting that fraudulent claims that are being rejected by councils are not being reported to the police. This means that unlike other crimes, there is no risk in trying to commit fraud, as unsuccessful attempts do not result in police attention or prosecutions. This is markedly different to other crimes, such as robbery, where even a failed attempt is likely to be reported to the police.

Central government should diversify the metrics by which they measure the ability of local councils to aid businesses. Just as government departments have been encouraged to increase the detection rate of fraud, so should local councils and this information should be made public too. Furthermore, practices such as sending cheques for grants should have been banned from the outset.

Coronavirus Business Interruption Loan Scheme (CBILS)[68]

- Available from 23 March 2020.
- Created for Small, Medium Enterprises (SMEs) to access finance.
- UK based businesses, with an annual turnover of up to £45 million who can prove that they have been negatively affected by coronavirus and would be viable under normal circumstances. Businesses must not have been classed as a 'business in difficulty' on 31 December 2019 in order to borrow in excess of £30,000.
- Eligible firms can borrow up to £5 million.
- Overdraft and invoice facilities are available for up to 3 years, while loans and asset finance facilities are available for up to 6 years.
- Loan 80 per cent guaranteed by the government, who also pay interest and fees for the first 12 months.
- 50 lenders are participating in the scheme (including all major retail banks). If rejected by one lender, can still apply to other lenders.
- Business must provide the lender with information regarding the size and length of the loan and what it will be used for. Further evidence, for example management accounts, cash flow forecasts, business plans, historic accounts and details of assets may be required.
- The lender had discretion as to whether to grant a loan, on the basis of the information provided.

67. Department for Business, Energy & Industrial Strategy, 'Grant Funding Scheme', May 2020, link

68. GOV.UK. 'Apply for the Coronavirus Business Interruption Loan Scheme', 2020, link

The fact that the CBILS is less susceptible to fraud is precisely the reason why it has been deemed unsuccessful in achieving its primary aim of providing emergency finance to SMEs, and why the riskier BBLS was deemed necessary. Additional checks by the lender to assess the verity of claims and viability of businesses seriously delayed the amount of time it took for a loan to be processed, undermining the speed that was necessary to keep businesses afloat in the current environment. As of 5th July 2020, only 50 per cent of CBILS had been approved, with £11.49 billion lent out to 53,536 firms.[69]

Coronavirus Job Retention Scheme[70]

- Available from 20 April 2020.
- Businesses can furlough their employees and apply for a grant to cover 80 per cent of their monthly wages, up to a maximum of £2,500 a month, plus National Insurance and pension contributions.
- Employers should receive compensation under the scheme within six working days.[71]
- Eligible for UK based firms for employees that have notified payment for an RTI submission to HMRC, on or before 19 March 2020. PAYE scheme reference number required for the application.
- Scheme available to cover the pay of full-time, part-time, casual, and shift workers.
- Furloughed workers must not undertake work for the employer.
- The scheme can be backdated to March 1 and will run until the end of October, with companies expected to contribute a greater share of wages from August.
- Employers cannot make more than one claim over the course of a claim period, so all employees to be furloughed over the claim period must be included in the initial application.

The Coronavirus Job Retention Scheme is the most expensive and most widely used Government support scheme, costing £27.4 billion and supporting 9.4 million jobs and over a million businesses as of 5th July 2020, and constituting approximately 40 per cent of the total economic package dedicated to COVID-19, according to the OBR.[72] The British Chambers of Commerce Coronavirus Business Impacts Tracker records that 70 per cent of surveyed firms had used the furlough scheme by May 2020, with 85 per cent of these firms having already received payment from the government under this scheme.[73] Within the first half an hour of the scheme being made available, 67,000 job claims had been made, with the system able to process up to 450,000 applications an hour.[74]

The sheer volume of claims and payments makes this scheme one of the schemes most susceptible to fraud, both in the UK and abroad. Jim Harra, head of HMRC has recognised that this scheme will be a 'target for organised crime', which is why HMRC laid out the following steps to minimise fraud:

69. HM Treasury, 'HM Treasury coronavirus (COVID-19) business loan scheme statistics', *GOV.UK* [website], accessed July 2020, link.

72. HMRC, 'HMRC coronavirus (COVID-19) statistics', *GOV.UK* [website], July 2020, link.

73. British Chambers of Commerce, 'Coronavirus Business Impacts Tracker, Week 8', accessed May 2020, Link

74. BBC, 'Coronavirus: More than 140,000 firms claim wage bill help', April 2020, Link

70. HM Government, 'Claim for your employees' wages through the Coronavirus Job Retention Scheme: A step by step guide for employers', 2020, Link

71. Bernal, N. 'The UK's coronavirus furlough scheme, explained by experts', Wired, May 2020. Link

- Only employees on the payroll before 19 March eligible
- Claims must be verified through an existing PAYE scheme
- Whistleblowing of employees forcing furloughed workers to work encouraged
- Selective checks to be performed by HMRC[75]

Similarly, addressing concerns about his furlough scheme in a twitter question and answer session in early April, the Chancellor Rishi Sunak said:

> *"We need to have some way of checking that people were actually employed by a company at this time... otherwise the whole system is open to an enormous fraud risk of just anybody saying that they would be working and could be furloughed. We need to be able to process these claims and verify these claims. The only way we have to do this is the payroll data.[76]"*

However, despite HMRC claiming to encourage whistleblowing, it took at least a month after the scheme was introduced for a page to be added to GOV.UK, where COVID-19 scheme related fraud could be reported. Prior to this, the link encouraging the reporting of such fraud led to a generic *Report Fraud to HMRC* site, which had not been altered to reflect the new types of fraud that had become possible due to COVID-19 support schemes (options were: Report Tax Fraud online; Report Customs, VAT or Excise Fraud Online; Benefit Thief; Fraudulent HMRC emails, text messages and suspicious phone calls; tax evasion). HMRC should do more to emphasise the fact that companies defrauding COVID-19 schemes are taking public money and it is in the public's direct interest to report them.

The reason why it is so important that the public can easily report furlough fraud is because the CJRS is one of the most difficult schemes to monitor. With at least 54 per cent of businesses utilising remote working, it is almost impossible to assess whether those on furlough are continuing to work from home.[77] This will become more problematic as restrictions are loosened allowing employees to resume part-time working. Monitoring whether an employee is working a three or four day working week is near impossible.

Furthermore, the Coronavirus Job Retention Scheme could still be defrauded in the following manner:

- Employers furloughing employees who continue to work for the company (where employees are specifically asked to continue working or where they have not been told that they have been furloughed).
- Employers paying furloughed employees less than the 80 per cent of wages paid for by HMRC.
- Employers falsely claiming wage subsidies for periods of time when the employee was working.
- Employers continuing to claim wages for staff who have terminated their employment, but who have not been removed from the payroll by 19 March 2020.

75. Chris Giles, 'HMRC Chief warns job retention scheme a target for organised crime', The Financial Times, April 2020, Link
76. The Sun, 'Work woes. Martin Lewis pleads with Chancellor Sunak to tweak furlough rules to help people who've lost new jobs', April 2020, link
77. Dixon, H. 'Half of people unable to work from home in coronavirus lockdown, figures suggest', The Telegraph, April 2020, Link

Policy Exchange has also received the following anonymous reports of furlough fraud:

- An employee handed in their notice at a pub at the beginning of March to go travelling in April. When travel plans were cancelled, the pub owner offered to furlough the employee as they had not yet been removed from the payroll.
- An employee has continued to work reduced hours, handling customer service queries from home after being furloughed.

1,868 cases of furlough fraud had been reported to HMRC as of 29 May 2020 and two charities, Protect and Whistleblowers UK, have raised concerns about the extent of furlough fraud being perpetrated.[78] Companies which have made headlines for pressuring furloughed employees to work include Sports Direct and House of Fraser.[79]

The Government should respond swiftly and publicly to claims of fraud, to reassure the public that this continues to be a priority and set an example that this is unacceptable behaviour. HMRC appears to be laying the groundwork for such action, publishing draft legislation that will alter the Finance Bill 2020. According to this legislation, HMRC will reclaim fraudulent CJRS and SEISS claims through Income Tax assessments and will 'charge a penalty in cases of deliberate non-compliance'.[80] Furthermore, directors are to be held jointly responsible for cases of furlough fraud. The consultation for this draft legislation will close on 12 June 2020. It will however take weeks for this to come into effect, minimising the deterrent effect of such legislation as it will only be effective for the latter half of the lifespan of the furlough scheme.

Some academics also believe that a higher rate of fraud than the 0.5 per cent to 5 per cent range usually applied by the Government is more realistic for such employment support schemes. Friedrich Schneider, an economics professor at Johannes Kepler University, Linz, believes that the German *Kurzarbeit* scheme will lose between 8 and 10 per cent of payments to fraud.[81] Considering the significant cost of the CJRS, it is particularly alarming that it is likely to have such a high fraud rate. If the CJRS suffers from this rate of fraud, the Government will lose an additional £2.7 billion to fraud.

78. Jo Faragher, 'Almost 1,900 reports of furlough fraud to HMRC', Personnel Today, June 2020, Link
79. Jonathan Paige, 'Coronavirus: Sports Direct 'pressured furloughed staff to work'', The Times, May 2020, Link
80. HMRC, 'Corporation Tax/Income Tax - Taxation of Coronavirus Support Payments', May 2020, Link
81. Martin Arnold, 'Furlough fraud plagues Europe's drive to save jobs from pandemic', Financial Times, May 2020, link

Self-Employment Income Support Scheme

- Allows the self-employed to claim 80 per cent of their average monthly trading profits
- The grant does not need to be repaid, however is subject to Income Tax and self-employed National Insurance.
- The grant must be below £7,500 and is paid out in a single 3 month instalment.
- Those eligible must have traded in the tax year 2018-19 and submitted a Self Assessment tax return on or before 23 April 2020 for that year, have traded in the tax year 2019-20, intend to continue to trade in the tax year 2020-21, have trading profits that do not exceed £50,000 and pursue a trade that is negatively impacted by coronavirus.
- Eligibility will first be assessed on the basis of the 2018-19 Self Assessment tax return, with tax returns from 2016 onwards used as supplementary evidence for those who do not appear initially eligible.
- It is expected that 95 per cent of the self-employed will be covered by this scheme.

As of the 5th July 2020, £7.7 billion worth of claims had been made by 2.7 million people.[82] When the Chancellor introduced the package of measures for the self employed, he acknowledged that his measures might be attractive to those looking to perpetrate fraud.[83] This is why HMRC decided to use existing information to contact those who are eligible, minimising the risk of fraud for this scheme. Nevertheless, some risk remains, as those contacted by HMRC must present evidence that their business has been adversely affected by COVID-19, which could result in over-exaggerated claims.

Universal Credit

The Department for Work and Pensions defines benefit fraud as cases where all three of the conditions listed below apply:

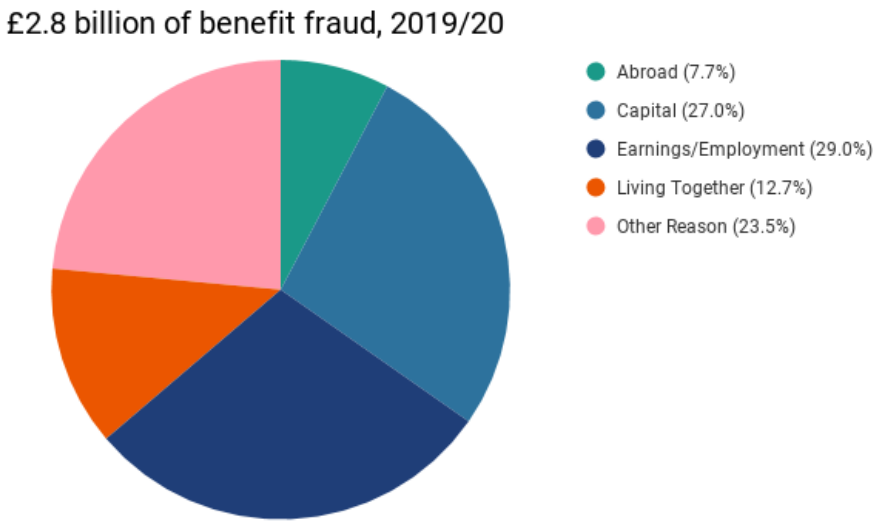
- The conditions for receipt of benefit, or the rate of benefit in payment, are not being met;
- The claimant can reasonably be expected to be aware of the effect on entitlement;
- Benefit stops or reduces as a result of the review.[84]

82. HMRC coronavirus (COVID-19) statistics, *GOV.UK* [website], July 2020, link.

83. Geroge Parker, Jim Pickard, Chris Giles, 'Rishi Sunak unveils rescue package for self-employed workers', The Financial Times, 26 March 2020, link

84. Department for Work and Pensions, 'Fraud and Error in the Benefit System: Latest data from DWP for Great Britain in 2019-20'. Link

Figure 4: Breakdown of benefit fraud in 2019/20 into 5 different typologies.[85]



Benefit fraud has been - and remains - a priority for the Department of Work and Pensions. In 2019-20, £2.8 billion was lost to benefit fraud, or the equivalent of giving each benefit claimant an additional £140 a year.[86] The fraud rate is highest for Universal Credit, which was 7.6 per cent of total expenditure compared to the average fraud rate for all benefits of 1.4 per cent.[87] Indeed, almost 1 in 5 Universal Credit applications are fraudulent. This is why a doubling of expenditure on Universal Credit between 2018/19 and 2019/20 has been used to explain the overpayment rate for all benefits increasing from 2.1 per cent to 2.4 per cent.[88] This has a severe financial impact on the public sector and on the delivery of Universal Credit.

This is why the DWP has a specialist system to detect fraud and error, called RIS (Risk Intelligence System). It also runs a scheme called IRIS (Integrated Risk and Intelligence Service) - a central function for analysing data and intelligence on fraud and error.

85. Department for Work and Pensions, 'Fraud and Error in the Benefit System: Latest data from DWP for Great Britain in 2019-20'. Link
86. Based on there being 20 million benefit claimants, as of August 2019. DWP National Statistics, 'DWP benefits statistical summary', February 2020, Link.
87. Department for Work and Pensions, 'Fraud and Error in the Benefit System 2019/20', link
88. Department for Work and Pensions, 'Fraud and Error in the Benefit System 2019/20', link

Universal Credit (UC)[89]

- Universal Credit is a single monthly payment to help those on a low income or the unemployed with living costs.
- For people based in the UK, over the age of 18 (some exemptions for 16 and 17 year olds) but under the State Pension age, with less than £16,000 in savings between yourself and your partner.
- Universal Credit for the unemployed consists of the following standard allowance, with additional payments for those with children (£235.83 per child), a disability that prevents work (£341.92), provide care for at least 35 hours a week for a severely disabled person who receives UC (£162.92) and for housing costs. This includes the £20 a week uplift in UC announced by the Chancellor as a result of the coronavirus crisis.

Circumstances	Monthly Standard Allowance
Single and under 25	£342.72
Single and 25 or over	£409.89
In a couple and you're both under 25	£488.59 (for you both)
In a couple and either of you are 25 or over	£594.04

- Universal Credit for the employed is tapered, so that for every £1 you earn, your UC
- payment is reduced by 63p. Those looking after a child or with a disability that affects their ability to work are eligible for a 'work allowance'. This allows them to earn £512 a month (£292 if they receive help with housing costs) before their UC payments are tapered.
- A surplus earning equal or greater than £2,500 more than the limit at which UC payments are stopped will be counted towards the following month's earnings.
- For the self-employed, both losses and surplus can be carried forward into the following month.
- Usually takes around 5 weeks for the first UC allowance to be paid out, which consists of a 4 week assessment period and an additional 7 days for the payment to be made.
- Applicants in need can receive a sum equal to their first estimated payment as an advance, which is paid back out of subsequent UC payments.
- UC claimants must engage in activities such as looking and applying for jobs or being trained, agreed in a 'Claimant Commitment'. Those who fail to adhere to the Claimant Commitment will see their UC payments stopped or reduced (a sanction).

In light of the fact that there have been two million new claims for Universal Credit as a result of the COVID-19 crisis, this is an area of government spending that is particularly vulnerable to fraud. Changes to UC as a result of COVID-19 that increase UC average payments, make fraud even more attractive:

89. GOV.UK. Universal Credit. Accessed May 2020. Link

- Claimants will no longer receive a sanction for failing to keep to their Claimant Commitment and do not have to attend jobcentre appointments until at least the 19th June.[90]
- Face-to-face assessments for health and disability-related claims have been suspended.
- The Standard Allowance has been increased by £20 a week.
- Local Housing Allowance rates have been increased to cover up to 30 per cent of market rent.
- The Minimum Income Floor for the self-employed has been relaxed for the duration of the coronavirus outbreak.

The impact of suspending face-to-face assessments will have a large impact on UC fraud rates in this crisis, evident in the varying fraud rates that resulted from a previous DWP decision to remove face-to-face assessments for claimants wishing to access advance payments. A National Audit Office investigation into UC advances fraud found that the monthly referrals of suspected advance fraud cases jumped from 179 in July 2018 to 15,044 in July 2019 as a result of the introduction of online applications and assessments. In mid-September 2019, DWP made a face-to-face interview a requirement for claimants to receive an online advance. Since then, the number of suspected advance fraud cases has fallen again to just over 2,000 in December 2019. The National Audit Office believes that up to £150 million may have been lost to this type of fraud.[91] We must therefore not underestimate the effect that suspending face-to-face assessments will have on the number of fraudulent UC claims over the course of this crisis.

Furthermore, the rapid rate at which new applications to UC have been made has exacerbated the risk of fraud, with the DWP experiencing six times the usual application rate between 16 March and 9 April 2020.[92] Despite these enormous pressures, DWP paid out 93 per cent of claims processed in the first week of the emergency lockdown restrictions on time. In order to continue processing the high volume of payments on time, some procedures have had to be relaxed and staff who usually work on fraud for DWP have been diverted to deal with the influx of new claims. The following changes have been applied to the processing of UC claims, to handle the increased number of claims:

- Applicants no longer need to call DWP to schedule an appointment.
- Applicants affected by COVID-19 can receive a month's advance upfront, without having to physically attend a jobcentre.
- The self-employed do not have to demonstrate 'gainful self-employment' when making a UC application.[93]
- Some information, such as housing costs, has been taken on trust.[94]
- It may well be the case that civil servants working on UC fraud have been redirected towards UC delivery due to the numbers of people applying for Government benefits.

90. Department for Work and Pensions, 'Coronavirus and claiming benefits', May 2020, Link
91. National Audit Office, 'Universal Credit advances fraud', March 2020, link
92. Department for Work and Pensions, 'Official Statistics, Universal Credit: 29 April 2013 to 9 April 2020', May 2020, link
93. Department for Work and Pensions, 'Coronavirus and claiming benefits', May 2020, Link
94. BBC News, 'Coronavirus: Benefit claims fraud could be £1.5bn', May 2020, link

While DWP have naturally been keen to emphasise the rate at which they have been able to process claims, especially given the inability of the programme to do so in the past, this has come at a cost. Policy Exchange has received reports of mass fraud, of around 25 to 30 per cent of the applications that some employees are dealing with, as a result of relaxing due diligence.

International Examples of COVID-Related Fraud

Governments across the world have been struggling to prevent cases of COVID-19 fraud. In the US, the Attorney General urged the public to report accusations of COVID-19-related fraud to the National Center for Disaster Fraud (NCDF) hotline, including attempts at private sector fraud (e.g. phishing emails posing as WHO; fake cures for coronavirus and medical providers using information obtained from COVID-19 tests to fraudulently bill for other services).[95] He also directed "all US attorneys to prioritise the investigation and prosecution of Coronavirus-related fraud schemes".[96]

These measures have done little to stem the tide of organised public sector fraud in the US. For instance, a Nigerian serious and organised crime group is alleged to have stolen "hundreds of millions of dollars of unemployment benefits from Washington state"[97] during the pandemic. Using stolen information, the criminals filed tens of thousands of fraudulent unemployment benefit claims at a time when the system was overloaded with legitimate applications.

Germany has also struggled, with authorities vowing to address COVID-19 related fraud after mounting evidence emerged that fraudsters were exploiting the country's aid programme for businesses. Hubertus Heil, labour minister, said:

> *"Most people will behave decently and the black sheep that are committing fraud, we will catch them, and we will punish them."*[98]

In one example of fraud, criminals created more than 90 fake websites that trawled the data of companies applying for emergency state funds, before then using the information to apply for funds from the state.[99] One state in Germany, North Rhine-Westphalia suspended its aid programme after discovering that criminals had defrauded hundreds of thousands of euros using the fake sites.

In Australia, the Treasury has confirmed that it:

> *"will be working with the ATO and the Australian Federal Police taskforce in investigating any cases of fraud related to the government's COVID-19 stimulus measures"*[100]

Amongst other measures, the Office of the Independent Commissioner Against Corruption has also issued advice for public officials on "Fraud and the COVID-19 Stimulus Package".[101]

On 21 May, Italian police arrested Sicily's coronavirus coordinator Antonio Candela and nine other health care officials for bribery and

95. Norton Rose Fulbright, 'US Department of Justice launches new COVID-19 anti-fraud initiative', March 2020, live
96. U.S. Department of Justice, 'Attorney General P. Barr Urges American Public to Report COVID-19 Fraud', March 2020, link
97. Richard Hall, 'Nigerian fraud ring exploits coronavirus crisis to scam 'hundreds of millions' in unemployment benefit from Americans', May 2020, link
98. Guy Chazan, 'Germany cracks down on coronavirus aid fraud', April 2020, link
99. Guy Chazan, 'Germany cracks down on coronavirus aid fraud', April 2020, link
100. Lian, J. 'AFP teams up with ATO, Treasury in COVID_19 tax fraud taskforce', Accountants Daily, April 2020, link
101. Office of the Independent Commissioner Against Corruption, 'Fraud and the COVID-19 Stimulus Package - Advice for public officials', April 2020, link

corruption linked to the purchase of medical equipment and service contracts valued at £540m connected to the mafia.[102]

> *"Col Gianluca Angelini of the financial police said they had discovered "a true centre of power… in which dishonest public officials, unscrupulous businessmen and entrepreneurs are willing to do anything to obtain contracts worth millions".*

In France the *chômage partiel* (partial activity) scheme, which supports the wages of around 12.3 million workers, has been exploited by firms inflating their wage claims and also forcing furloughed employees to work. Inspections of nearly 2,000 Austrian companies found 460 firms breaching the terms of the Autrian *Corona-Kurzarbeit* (Corona short-term work) scheme.[103]

Canada has also suffered from benefit fraud. Canada's labour-force survey, which was completed on the 18th April 2020, indicated that there were 5.5 million eligible for the Canada Emergency Response Benefit, but by the 19th April 2020, there had been 6.7 million claims for the benefit. While the discrepancy is in part due to statistical error, fraud undoubtedly played a role in this too.[104]

These examples highlight the scale of the challenge for governments attempting to address public sector fraud as a result of their response to the pandemic. They serve as a warning that new measures will need to be introduced by governments if they are to succeed in preventing large scale public sector fraud linked to the pandemic and in particular, abuse of the government subsidy schemes designed to support employees and businesses and prevent large scale unemployment. Ultimately, governments should learn from this experience and increase the range of preventative measures and financial controls in place that are specifically designed for disaster scenarios, so that they are better prepared for the next crisis.

Measures that need to be introduced include widespread government awareness campaigns to alert the public sector to the possibility and risks of fraud and to enlist the assistance of the public in reporting fraud. In addition, new monitoring systems will need to be established across government departments to ensure that counter fraud measures are joined up and that new fraud methodologies are spotted quickly and dealt with. It will also be necessary for governments to investigate and prosecute COVID-19 crimes to maintain the confidence of their populations funding the schemes being defrauded. To do otherwise will risk threatening the sense of national unity and purpose that has emerged during the crisis.

102. BBC, 'Italy bribery probe nets Sicily coronavirus response chief', May 2020, link
103. Arnold, M. 'Furlough fraud plagues Europe's drive to save jobs from pandemic', Financial Times, May 2020, Link
104. Tom Blackwell, *'Number of CERB claimants topped number of jobless by a million last month, statistics show'*. National Post, May 2020, Link

3. The Impact Of Fraud

The Effect of Fraud on the Economy and Its Victims

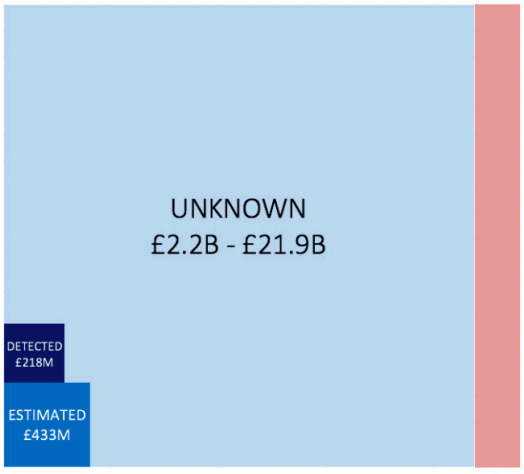
As with all crime, fraud has a range of costs. The first is the economic cost, which occurs directly as a result of the crime. The second is the psychological and physical cost, borne by victims and individuals subjected to the crime. The third is specific to public sector fraud and is the cost to society of trust in public sector organisations and institutions being eroded by the inability of the government to protect the public finances.

Economic Impact of Fraud

There are a range of estimates for the cost of fraud, with some studies (e.g. Button et al. (2017)) suggesting that the aggregate cost of fraud to the UK could be as high as £190 billion a year.[105]

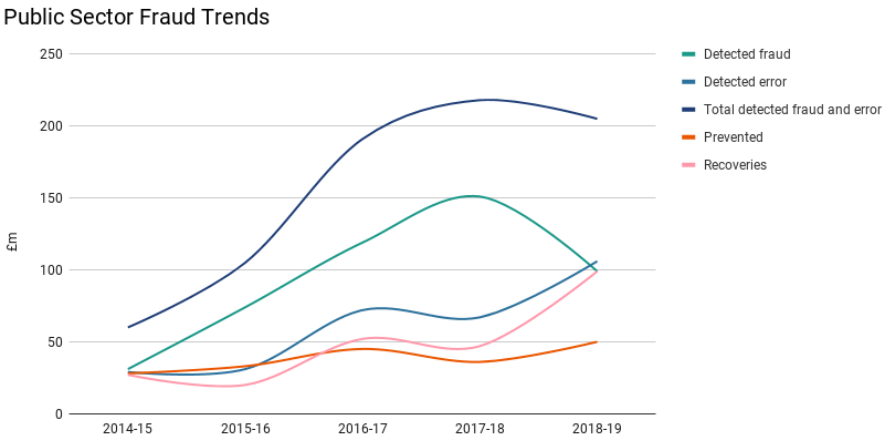
The government has acknowledged that in 2017-18, between £2.8 billion and £22.6 billion was lost to fraud and error, outside the tax and welfare system.[106] This can be broken down into detected fraud, estimated fraud and unknown fraud (Figure 5). The Cabinet Office arrives at this estimate by estimating the cost of public sector fraud and error at 0.5 per cent - 5 per cent of public spending. They have produced a range to reflect the hidden nature of fraud and difficulty in identifying it, as well as reflecting the levels of fraud risk faced by different government departments. This estimate has been informed by 53 loss measurement exercises undertaken over the last five years by the Fraud Measurement and Assurance Programme.[107]

Figure 5: Scale of Public Sector Fraud in the UK in 2017-18 (excluding fraud in the tax and welfare system).[108]



105. Police Foundation, 'More than just a number - improving the police response to fraud', 2018, link
106. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link
107. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link
108. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

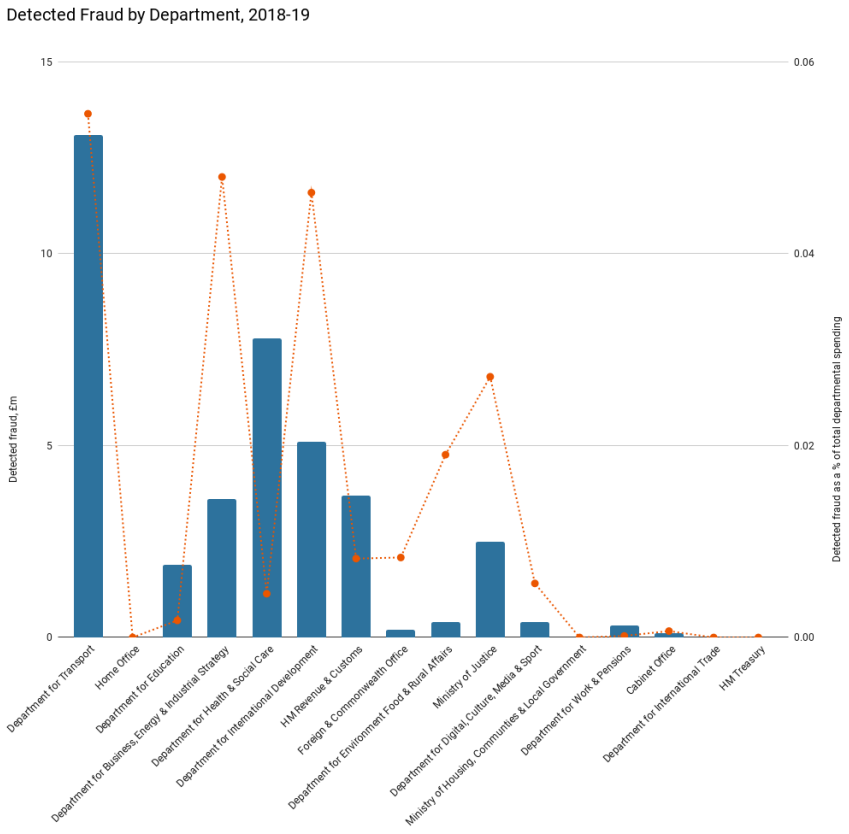
Figure 6: Trends in detected, prevented and recovered public sector fraud since 2014.[109]



During the past decade the UK Government has made a concerted effort to improve the detection and prevention of fraud, a trend evident in the steady rise of total detected fraud and error between 2014 and 2018 (Figure 6). Prevention has been recognised as the most effective way to address fraud, but this is not possible without information and knowledge about the type and scale of fraud being committed.[110] This is why investment in data analytics and fraud detection is vital as a first step to ensuring fraud prevention becomes ingrained into government systems, practices and policy with effective counter fraud solutions continuing to be developed. An increase in the detection of fraud, as highlighted in Figure 6, should be seen as a positive development. Furthermore, when looking at the increase in prevented and recovered fraud, which may appear modest, it must be borne in mind that the public sector is at the start of a process involving a total shift in approach to fraud and that the positive uptake in both these indicators highlight the gains available from adequately investing in combating fraud.

109. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link
110. 'International Public Sector Fraud Forum, 'A guide to managing fraud for public bodies', February 2019, link

Figure 7: Detected fraud by departments in £m and as a per cent of total spending. We have excluded the Ministry of Defence, as their detected fraud was artificially high, as this included the outcome of a three year fraud spend audit in defence spending[111]



There were 10,116 reported allegations of suspected fraud by Government departments in 2018-19.[112] Comparing public sector fraud by department is important as most public sector fraud is prevented and detected at the departmental level and despite the traditional focus on fraud in the tax and welfare system, all departments are at risk (Figure 7). This diagram shows that the apparent success of some departments who initially appear to be effective at detecting fraud is overstated when compared to their total spending. For example, it appears that the Department for Health and Social Care has detected relatively high levels of fraud (£7.8m) compared to the Department for Business, Energy & Industrial Strategy (£3.6m). However, considering the DHSC's significantly larger budget (£171bn vs. £7.5bn for BEIS), it can be seen that it has a relatively low detection rate. It is important that public sector fraud reviews, such as *The Cabinet Office Fraud Landscape Annual Report*, include more information that allow for more accurate monitoring of progress and comparisons between departments.

When discussing the economic cost of fraud, it is also important to note the economic cost of instituting measures to counter fraud. Tackling fraud undoubtedly requires a continuous investment of both time and

111. Institute for Government, 'Total managed expenditure (TME) by department 2018-2019', 2020, link; Cabinet Office,'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

112. Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

resources. Fraud creates additional costs, such as to prisons and the CPS, that drain resources from a range of Government departments. It is welcome that the Government has committed £48 million over 2019/20 to fight economic crime.[113] However, the process of preventing, detecting and recovering fraud can be painstaking and require unique investigative skills. Outcomes that can result include pay-offs that are either intangible or only materialise in the long term. When there is additional pressure on public expenditure (as can be expected in the aftermath of the COVID-19 crisis), it can be difficult for departments to justify investment in counter fraud measures, the success of which cannot be accurately measured. It is also vital to recognise that fraudsters are continuously altering and adapting their methodologies and techniques. Constant vigilance is required by the government if fraud is to be detected and countered. As long as a public sector exists, there will be people trying to defraud it. The only way the government can hope to minimise this is through continuous investment, regardless of the fiscal environment.

It must also be borne in mind that beyond the direct economic cost to the Government, public sector fraud has negative economic consequences for the recipients of Government services. If Government taxes are taken by criminals, populations suffer as resources are taken away from essential services such as the NHS, schools, and law enforcement. Furthermore, when taxes are taken fraudulently by criminals, especially by organised crime networks, the proceeds are sometimes used to fund damaging activities such as terrorism and harmful organised criminality such as drug supply and human trafficking. For instance, a man in Berlin who attempted to defraud the German Government of €18,000 earmarked for businesses suffering from the COVID-19 crisis has been found to have links to militant Islamist movements.[114]

Pervasive fraud can eventually even prevent governments from offering services altogether. For example, high levels of fraud in the German North Rhine-Westphalia COVID-19 aid programme forced the government to suspend all aid for a week.[115] This means that those who needed the services most, as well as the criminals, were starved of funds.

The Reporting and Recording of Public Sector Fraud

Fraud is notorious for being one of the most difficult crimes to gather accurate information on which is largely due to persistent underreporting of fraud and issues relating to the recording of fraud. The Crime Survey for England and Wales revealed that in 2019, 36 per cent of incidents of crime experienced by respondents was fraud, but only 13 per cent of police recorded crime for the same period was fraud.[116]

Firstly, not all victims are aware that they have been defrauded. For example, a DWP employee who does not recognise a fraudulent UC claim cannot report it. Secondly, those who do realise that they have become a victim of fraud often choose not to report it. There are two reasons for this. The first main reason is that victims do not bother to report frauds either because it is a small amount, or they do not feel the investigative

113. HM Treasury & Home Office, 'Economic Crime Plan 2019-2022', September 2019, link
114. Guy Chazan, 'Germany cracks down on coronavirus aid fraud'. Financial Times, April 2020, Link
115. Guy Chazan, 'Germany cracks down on coronavirus aid fraud', Financial Times, April 2020, Link
116. Office for National Statistics (ONS), 'Crime Survey for England and Wales, year ending in December 2019'. April 2020, Link

resources are in place to respond to the crime. This is particularly true of local authorities. The second less likely reason is a stigma that exists linked to fraud, where victims feel and are sometimes treated as though they are partly to blame for the crime[117]. This is because many acts of fraud require the victim to co-operate to some degree, by for example clicking on a link in an email or processing a fraudulent UC claim. Victims can therefore feel guilt, shame and embarrassment, which prevents them from reporting the crime. This problem is particularly acute in the public sector, where employees may feel that by reporting a fraud they have been victim to will impact the perception of them as a competent employee and may consequently affect their career progression in the future.

It is recommended that government departments reassure employees that there is strict confidentiality in the reporting of fraud.

Even when cases have been flagged as potentially fraudulent, it is not always clear whether this is as a result of an individual making an error, or is a case of fraud. For example, it is difficult to ascertain whether an NHS nurse who overstated their hours worked did so accidentally (especially when they are doing a lot of overtime) or intentionally. The Cabinet Office acknowledges this problem, urging departments to record fraud '*where the department judges that the misrepresentation, omission or abuse of position has been made fraudulently on the balance of probabilities*' and that '*action or inaction was more likely than not to have been to defraud the department rather than being erroneous*'.[118] As cases of fraud must not be proved to a criminal standard, this can lead to inconsistencies as different fraud officials in different departments judge cases more or less harshly.[119]

This is why some organisations only report data for 'fraud', whereas others report data for 'fraud and error'. Error encapsulates the overpayments which have been judged to have occurred as a mistake, as opposed to with malicious intent. While this allows officials to report data without having to make a judgement, the resulting figure is not accurate enough to gain a better understanding of fraud.

Even when fraud has been reported and confirmed, there are further problems with regards to the incentives to reporting public sector fraud. The government relies on data provided by individual departments, however it is not in the direct interest of departments to report high levels of fraud. Although detecting fraud is the first vital step in the fight against fraud, reporting fraud also attracts negative media attention. Therefore although the government has made it's objective to discover more fraud, the incentive to do so has not fully trickled down to the departments who must actually detect it. Although there have been improvements in fraud reporting indicative of culture change (21 per cent increase in the number of allegations of suspected fraud between 2017-18 and 2018-19), detected fraud is still significantly lower than estimated and unknown fraud (see Figure 1).[120]

Further confusion can arise around instances where there is no reported fraud (e.g. in Figure 7, the Home Office reports £0 fraud). Whilst at first glance it may appear that a department is highly effective at preventing

117. M. Button, C. Lewis & J. Tapley, 'Fraud typologies and victims of fraud', Centre for Counter Fraud Studies, Institute of Criminal Justice Studies, University of Plymouth, 2009, Link

118. Cabinet Office, 'Common areas of spend, Fraud, error and debt, Standard Definition v2.1', July 2014, link

119. Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

120. Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

fraud, it is often a sign that the resources and mechanisms required to detect fraud are not in place and that fraud is occuring undetected. Distinguishing between these two ends of the spectrum is difficult, but the introduction of the Counter Fraud Functional Standard (GovS 013), which outlines 12 procedures departments should have in place to fight fraud, in October 2018 should help mitigate this risk. As over the course of 2018-19, 90 per cent of departments and 84 per cent of arms length bodies met this functional standard, we can expect to see the number of departments detecting zero fraud to decline.[121]

Psychological and Physical Impact of Fraud

The ONS believe that in 2018, there were 3.8 million cases of fraud in England and Wales and it is therefore important not to lose sight of the psychological cost of fraud, given the high number of victims.[122] This is also true of public sector fraud, because although the Government is the target of the attack, all cases of fraud involve individuals, whether it is an official who has unknowingly co-operated, the individual who must deal with the fall out of the fraud or those who must continue to provide public services despite the necessary equipment or resources having been taken by fraudsters.

The financial hit from fraud can itself exacerbate stress. Research has found that 45 per cent of fraud victims felt that the financial loss they experienced had an impact on their emotional wellbeing and 37 per cent reported significant psychological or emotional impact.[123] As highlighted above, the varying levels of co-operation that victims are coerced into with an act of fraud can leave many victims with feelings of guilt, shame and distress.[124] The reputational damage for some victims of being involved in a case of fraud can be severe, especially with regards to employment prospects. Furthermore, the time spent trying to reclaim some of the costs of fraud can create additional stress and financial cost to victims.

Fraud in the NHS specifically can have a direct impact on people's physical health. For example, faulty PPE leaves nurses vulnerable to COVID-19, while the cost of fraud which is borne by the NHS reduces the quality of services that can be provided to patients. More widely, the fraud that is often present in infrastructure projects can have devastating impacts. It is being investigated whether the collapse of the Morandi bridge in Italy, which resulted in 43 deaths, was in part due to rampant corruption and fraud in the Italian construction industry.[125]

Societal Impact of Fraud

Fraud also has wider implications for Britain, for domestic society and for Britain's role as a global power. According to a PwC Global Economic Crime Survey, fraud is particularly damaging to '*reputation, brand and employee morale*'.[126]

High levels of public sector fraud implies that the Government cannot be trusted to handle public sector finances, and essentially people's hard earned taxes. Fraud therefore erodes public trust in the Government, and

121. Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link
122. Office for National Statistics, 'Crime in England and Wales: Additional Tables on Fraud and Cybercrime', April 2019, link
123. Police Foundation, 'More than just a number - improving the police response to fraud', 2018, link
124. International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', February 2020, Link
125. The Conversation,'Genoa bridge collapse: the mafia's role', August 2018, Link
126. International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', February 2020, Link

has the potential to create a crisis of confidence in the public sector. This can have a range of negative impacts, as it turns civil society away from engaging with the Government and the democratic process and weakens compliance with the law. It also affects the morale of Government employees, affecting compliance with anti-fraud measures, especially if the problem is seen as pervasive, as well as affecting their productivity.

Fraud also poses a national security risk, as it damages the reputation of Britain as a safe and secure country. This can affect the likeliness of other nations to share sensitive information with Britain, confirmed by the U.S. Secretary of State Mike Pompeo, who asserted that the US would only share information with the UK over 'trusted networks'.[127] Although this statement relates to Huawei and China, it highlights the threat to national security of a Government whose operations and systems appear vulnerable to interference and attack from third parties. This damage to Britain's international reputation also undermines British soft power and therefore its ability to gain support from other nations.

Furthermore, it negatively impacts the integrity and reputation of the UK's financial services sector, even making it a target for future attacks.[128] In light of the key role that the British financial sector will play in the success of Britain after Brexit, it is therefore vital that the reputation of this sector remains intact.

127. Henry Ridgwell, 'US Warns Information-Sharing at Risk as Britain Approves Huawei 5G Rollout', VOA News, January 2020, Link

128. HM Government & UK Finance, Economic Crime Plan, 2019-22, July 2019, link

4. UK Government Counter Fraud Measures

How the UK Government Fights Fraud

Responsibility for Government policy on *public sector fraud* rests in the Cabinet Office which is responsible for the counter fraud 'profession' and its function across the public sector. As part of the drive to improve fraud detection and prevention across Government, the counter fraud functional standard (GovS 013) was launched in October 2018. Of the 19 government departments and 36 arms-length bodies assessed in 2018/19 for their overall compliance level with these standards, 90 per cent of departments and 84 per cent of arms-length bodies were found to have met these standards.[129]

Government Counter Fraud Function

The counter fraud function is one of 14 functions across government that have been designed to improve the efficiency and effectiveness of the public sector. This function brings together over 15,000 public servants to fight public sector fraud by improving intelligence sharing across government, increasing understanding of the threat and improving fraud detection and prevention capabilities.[130] It advocates 12 steps to be implemented across government organisations:

1. Have an accountable individual at board level responsible for counter fraud, bribery and corruption.
2. Have a counter fraud, bribery and corruption strategy that is submitted to the centre.
3. Have a fraud, bribery and corruption risk assessment that is submitted to the centre.
4. Have a policy and response plan for dealing with potential instances of fraud, bribery and corruption.
5. Have an annual action plan that summarises key actions to improve capability, activity and resilience in that year.
6. Have outcome based metrics summarising what outcomes they are seeking to achieve that year. For organisations with 'significant investment' in counter fraud or 'significant estimated' fraud loss, these will include metrics with a financial impact.

129. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

130. 'Counter-Fraud Standards and Profession', *GOV.UK* [website], link, (accessed June 2020).

7. Have well established and documented reporting routes for staff, contractors and members of the public to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations.
8. Will report identified loss from fraud, bribery, corruption and error, and associated recoveries, to the centre in line with the agreed government definitions.
9. Have agreed access to trained investigators that meet the agreed public sector skill standard.
10. Undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels, including loss measurement activity where suitable.
11. Ensure all staff have access to and undertake fraud awareness, bribery and corruption training as appropriate to their role.
12. Have policies and registers for gifts and hospitality and conflicts of interest.[131]

While these standards are an important step in improving counter fraud capabilities across government, it is recommended that the following additional steps are taken:

1. This individual should report annually about the measures being taken to detect and combat fraud as well as new fraud threats.
2. Fraud, bribery and corruption risk assessments should be undertaken every other year, in light of the constantly evolving nature of the risk. In light of the new risk assessments, the strategy should be updated at the same intervals too.
3. Data should be published on the outcome of reports to improve follow up.

Furthermore, as the standards become ingrained in the operations of Government organisations, there should be an effort to continually update and improve the standards, so that they reflect the challenges of the evolving fraud landscape.

Additionally, all major Government departments have dedicated units that investigate fraud related to their government functions (see Figure 8 for a breakdown of fraud fighting bodies across Government):

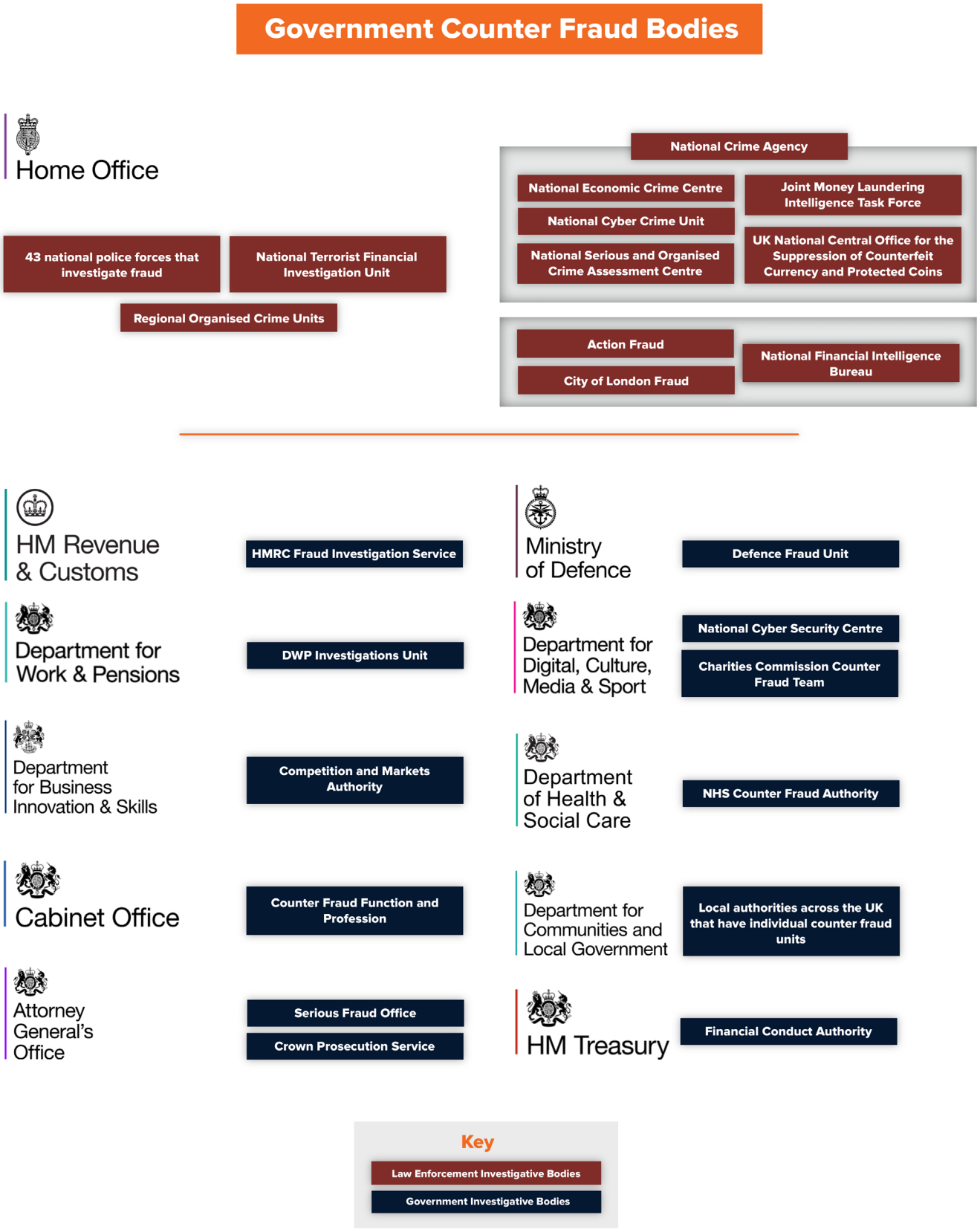
- **Her Majesty's Treasury (HMT)** that oversees the independent "Financial Conduct Authority (FCA);
- **Her Majesty's Revenue and Customs** (HMRC) has its own "HMRC Fraud Investigation Service";
- **Department of Health and Social Care** that has its own "NHS Counter Fraud Authority";
- **Attorney General's Office (AGO)** that presides over the Crown Prosecution Service (CPS) which prosecutes fraud investigations and the the Serious Fraud Office (SFO);

131. Cabinet Office, 'Cross-Government Fraud Landscape Annual Report 2019', February 2020, Link

- **Ministry of Housing, Communities and Local Government** that funds local authorities across the UK that have individual fraud investigation units;
- **Ministry of Defence** that has its own Defence Fraud unit;
- **Department of Digital, Culture, Media and Sport** that presides over the Charities Commission that has its own 'Charities Commission Counter Fraud Team';
- **Foreign and Commonwealth Office** that presides over GCHQ and the National Cyber Security Centre (NCSC);
- **Department for Work and Pensions** that has a "DWP Investigations Unit";
- **Department of Business Innovation and Skills** that oversees the independent non Ministerial Competition and Markets Authority (CMA)[132];
- **Home Office** that presides over the following investigative bodies:
  - National Crime Agency (NCA) which comprises two inter-integrated sub units:
    - National Economic Crime Centre (NECC)
      - Including the Joint Money Laundering Intelligence Task Force
    - National Cyber Crime Unit (NCCU)
  - National Terrorist Financial Investigation Unit (NTFIU) (a unit of the Counter Terrorism Command (SO15) within the Metropolitan Police
  - City of London (lead police force for fraud investigation) that is responsible for:
    - National Financial Intelligence Bureau (NFIB)
    - Action Fraud - national reporting centre for fraud
  - Regional Organised Crime Units (ROCUs) that investigate serious and organised fraud
  - 43 national police forces that investigate fraud

132. Competition and Markets Authority, 'About Us', *GOV.UK* [website], accessed May 2020, link

Figure 8: Counter fraud law enforcement and investigative bodies spanning the Government



This plethora of disparate fraud investigative and policy units across Government and law enforcement results in a lack of consistency and coherence in the overall effort to counter fraud. No single government department or Minister has full oversight or responsibility for 'fraud'. Accountability for outcomes is held by different Ministers with conflicting Ministerial priorities and objectives - resulting in a dilution of purpose, oversight, focus and accountability.

This is less so in the non governmental sector. A number of private and non governmental bodies assist with counter fraud policy and fraud investigation. These include:

- Cifas, a not-for-profit fraud prevention membership organisation;
- Chartered Institute of Public Finance and Accounting (CIPFA);
- UK Finance (a body representing the UK banking and finance industry);
- Fraud Advisory Panel, an independent charity and member organisation representing the voice of the anti-fraud community.

How the UK Government is fighting COVID-19 Public Sector Fraud

The UK Government responded fast to introduce a range of counter fraud and awareness raising preventative measures that preceded reports from various international bodies such as Interpol and the Financial Action Task Force (FATF) who sent global alerts early on in the crisis.[133]

The Cabinet Office (Government lead for the counter fraud profession) formed a COVID-19 Counter Fraud Response Team[134] to assist the government with its counter fraud response during the pandemic. The team published guidance on fraud control in emergency management[135], which sets out principles for public bodies in mitigating the risk of fraud. The guidance drew on the learning from the International Public Sector Fraud Forum (IPSFF)[136] publication 'Fraud in Emergency Management and Recovery Principles for Effective Fraud Control'[137] produced by the Cabinet Office and the Commonwealth Fraud Prevention Centre in February 2020.

In April, the government introduced guidance for individuals and business on fraud and cyber crime[138], separate guidance for leaders and fraud experts in government bodies and local authorities that are administering programmes on behalf of the UK Government[139] and has collaborated with the cross sector and cross industry Fraud Advisory Panel helping to establish the COVID-19 fraud watch group that has highlighted fraud risks, emerging issues and prevention tips[140].

The NHS Counter Fraud Authority issued 'COVID-19 counter fraud guidance'[141] that includes advice and guidance on COVID-19 related fraud risks faced by the NHS, with a focus on specific areas of risk and guidance on fraud against NHS staff.

The Charities Commission issued an alert on the 'increased risk fraud

133. FATF, 'Statement by the FATF President : COVID-19 and measures to combat illicit financing', April 2020, link
134. Government Counter Fraud Function 'COVID-19 Counter Fraud Response Team' accessed May 2020, link
135. Cabinet Office, 'Fraud control in emergency management: COVID-19 UK Government guide', March 2020, link
136. Consisting of senior representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States.
137. International Public Sector Fraud Forum, 'Fraud in Emergency Management and Recovery - Principles for Effective Fraud Control, February 2020, link
138. Home Office, 'Coronavirus (COVID-19): advice on how to protect yourself and your business from fraud and cyber crime, April 2020, link
139. Cabinet Office, 'Fraud control in emergency management: COVID-19 UK Government guide', March 2020, link
140. Fraud Advisory Panel, 'COVID-19 fraud watch', June 2020, link
141. NHS Counter Fraud Authority, 'Fraud prevention advice and guidance', May 2020, link

and cybercrime against charities'[142] on 17 April and engaged with the Fraud Advisory Panel in a webinar with sector partners to help spot COVID-19 related fraud and protect charities from harm.

The Home Office issued guidance[143] on 27th April on protecting individuals and businesses from fraud and cyber crime. The Crown Prosecution Service (CPS) issued guidance to police forces and prosecutors directing them that "all COVID-19 related cases" must be fed into the criminal justice system "immediately", including, for example, assaults on emergency workers[144].

The National Cyber Security Centre (NCSC) issued practical advice[145] on 8th April for individuals and organisations on how to deal with COVID-19 related malicious cyber activity.

These steps have helped to raise awareness of COVID-19 related fraud across government but more needs to be done now to ensure that frauds that have been undertaken during the crisis are properly investigated and prosecuted. This will require clear cross government lines of accountability, monitoring and co-ordination of all COVID-19 related public sector fraud investigations and strong leadership to ensure that frauds are not accepted as part of the cost of the overall crisis.

The Home Secretary and Chancellor of the Exchequer are jointly responsible for the Economic Crime Plan 2019-2022[146] that sets out seven priority areas that were agreed in January 2019 by the Economic Crime Strategic Board, the ministerial level public-private board charged with setting the UK's strategic priorities for combating economic crime. It is recommended that the recommendations set out in this plan are reviewed in light of the increase in fraud resulting from the COVID-19 crisis.

The Economic Crime Strategic Board[147] should also be reconvened to agree a co-ordinated response to the monitoring, investigation and prosecution of COVID-19 economic crimes across government to ensure adequate post event assurance for this crisis. A Minister for Fraud and Economic Crime should be appointed to oversee the prevention, detection, investigation and prosecution of all COVID-19 related frauds (public and private crime). This Minister should make a strong public and political commitment to addressing all public sector fraud relating to the COVID-19 crisis, seek cross party consensus and announce how public sector fraud will be monitored, investigated and prosecuted.

The lead Minister for Fraud and Economic Crime should appoint a single law enforcement lead (Deputy Director General of the NCA) to be responsible and nationally accountable for the prevention, detection, investigation and prosecution of COVID-19 related economic crimes. The Home Office and HMRC should fast track the review of Economic Crime Governance - an action from Economic Crime Plan (Sept 2019) in light of the anticipated scale of COVID-19 economic / fraud crime.

142. The Charity Commission, 'Coronavirus (COVID-19): increased risk of fraud and cybercrime against charities', April 2020, link
143. Home Office, 'Support for businesses and self-employed people during coronavirus', April 2020, link
144. Crown Prosecution Service, 'Interim CPS Charging Protocol - COVID-19 response', April 2020, link
145. National Cyber Security Centre, 'Advisory: COVID-19 exploited by malicious cyber actors', April 2020, link
146. HM Treasury & Home Office, 'Economic Crime Plan, 2019 to 2022', July 2019, link
147. HM Treasury & Home Office, 'Economic Crime Strategic Board January 2019 agenda and minutes', July 2019, link

Oversight, Governance and Accountability for Fraud

The COVID-19 crisis presents unique challenges to the oversight of both private and public sector fraud that cut across different government departments. The anticipated scale of public sector fraud committed against the Government alongside known COVID-19 related fraud against private individuals and the private sector necessitates greater Ministerial oversight and clear lines of operational accountability.

It is recommended, therefore, that the Home Secretary and Chancellor of the Exchequer should revisit the recommendations in the Economic Crime Plan 2019-2022[148] and reconvene the Economic Crime Strategic Board[149] to agree a co-ordinated response to the monitoring, investigation and prosecution of COVID-19 economic crimes / frauds across government

The Prime Minister should also create a new **Minister for Fraud and Economic Crime** (separate from the current portfolios of the Security Minister) to oversee the prevention, detection, investigation and prosecution of all fraud and economic crimes including COVID-19 related frauds (both private and public sector). This Ministerial portfolio should straddle both Home Office and Cabinet Office responsibilities in this area.

The lead Minister for Fraud and Economic Crime should appoint a single law enforcement lead (Director General of the NECC) to be responsible and nationally accountable for the prevention, detection, investigation and prosecution of COVID-19 related economic crimes across the entirety of the private and public sector.

This Minister for Fraud and Economic Crime should make a strong public and political commitment to addressing all public sector fraud relating to the COVID-19 crisis, seek cross party consensus and announce how public sector COVID-19 related economic crimes / frauds will be monitored, investigated and prosecuted. The Minister should also lead a COVID-19 fraud public awareness campaign encouraging the public to report crime related to COVID-19 - specifically addressing the perception that fraud is victimless.

A new Minister for Fraud and Economic Crime should explore whether some or all of the investigative units dealing with public sector fraud across the different Government departments should be brigaded under the oversight and operational leadership of the NECC in order to increase and improve operational capabilities to investigate fraud within both the public and private sector.

It is also recommended that the Home Office provide substantial additional funding to resource a new Ministerial post for Fraud and Economic Crime and to significantly uplift the operational capability of the NECC within the National Crime Agency so that it can lead operationally for all types of COVID-19 fraud across the public and private sector.

148. HM Treasury & Home Office, 'Economic Crime Plan 2019-2022', July 2019, link ,
149. HM Treasury & Home Office, 'Economic Crime Strategic Board 2019 agenda and minutes', July 2019, link

Leadership and Criminal Investigation of COVID-19 Related Fraud

UK Government initiatives to prevent COVID-19 criminality outlined above will not have stemmed an inevitable increase in public sector fraud but the extent of this remains unknown currently.

Anticipating that there has been and will likely continue to be a substantial increase in public sector fraud, the Government and law enforcement agencies now need to take stock, evaluate and assess fraudulent losses to the Government and undertake painstaking investigations to prosecute those who have committed fraud and recover the proceeds of the crimes.

This will be an extremely challenging undertaking as fraud investigation can be complex and time consuming and UK policing in particular is poorly equipped to investigate fraud in normal times. Fraud investigation has never before been a police priority and is one of the most under resourced and unskilled areas of UK policing. Most importantly, the COVID-19 fraud investigative challenge cuts across multiple government departments and law enforcement agencies. How then should a cross government effort ensure that this function is nationally coordinated with clear lines of accountability? In addition to clear Ministerial oversight and accountability, there is a need for clear operational leadership.

The National Economic Crime Centre (NECC) (established in October 2018) is a new body within the National Crime Agency (NCA) which was created following a review of economic crime by the Cabinet Office. Announced by the then Home Secretary Sajid Javid in December 2017, it is now:

> *"the national authority for the UK's operational response to economic crime, maximising the value of intelligence, and prioritising, tasking and coordinating to ensure the response achieves the greatest impact on the threat".*

At the outset of the COVID-19 crisis, the NECC established Project Etherin that aimed to 'understand, respond and communicate' the challenge of fraud related to the crisis. Daily meetings have been held between the NECC and Action Fraud, NFIB and other agencies, examining the almost 2,500 COVID-19 related fraud allegations (approximately 2 per cent of all fraud allegations) that have been reported since the start of the epidemic, leading to several law enforcement operations, arrests and seizures.

On public sector related fraud, the NECC has been working with the Cabinet Office on counter fraud advice, due diligence checks on new suppliers to the NHS, proactive analysis of Suspicious Activity Reports (SARS) and through joint work on investigations.

The NECC has also set up a COVID-19 fusion cell of thirty different organisations including major banks, UK finance law enforcement community, regulators, government departments, insurance industry etc.) to share information relating to the crisis.

It is recommended that the National Economic Crime Centre (NECC) within the NCA should formalise the creation of a '**COVID-19 Fraud**

Crime Hub' and **COVID-19 Fraud Crime Forum** to oversee and coordinate the prevention, detection, investigation and prosecution of COVID-19 related economic / fraud crimes across the entirety of the public sector of Government. This forum should share best practice and look to find synergies and overlaps between investigations. The sharing of investigative resources could also be a by-product of such a forum.

The NECC is ideally placed to also undertake a National Risk Assessment of COVID-19 economic crime and co-ordinate the prevention, detection, investigation and prosecution of COVID-19 related economic / fraud crimes across the UK government. It has the capability to understand the threat of COVID-19 fraud (using its new National Data Exploitation Capability) and devise an operational plan leading to the tasking of investigative bodies. Accountable to the Director General of the NCA and the Home Secretary, the NECC has the following key partners operating from within it: SFO, FCA, City of London Police, HMRC, CPS and the Home Office. It is:

> *"A truly collaborative, multi-agency centre that has been established to deliver a step change in the response to tackling economic crime"*[150].

Arguably, the COVID-19 fraud investigative challenge is the first real test of the NECC that was established to deal with cross government, law enforcement economic crime issues such as those that have evolved during the COVID-19 pandemic.

For serious and organised public sector COVID-19 fraud allegations, the NECC should ensure that the right investigative body is tasked to investigate, whether that is the NCA itself, the SFO, the City of London Fraud department or one of the Regional Organised Crime Groups (ROCUs).

A new Minister for Fraud and Economic Crime should instigate a substantial uplift in additional investigative resources to assist the investigation of major COVID-19 related fraud investigations (e.g. an uplift in the resources at the NECC, NHS Counter Fraud Authority, HMRC Fraud Investigative Service and DWP Investigations team).

Less major crimes will need to be tasked to government investigative teams or police forces in the normal way (through NFIB) but tasking needs to take account of the lack of a national fraud policing strategy and poor investigative skills across police forces for investigating fraud and economic crimes. A recent review by Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS)[151] found that:

> *"the scale and reach of fraud challenges the local policing model, that local and regional policing structures are inadequate, and dedicated fraud resources are, at best, limited in number. There is an inadequate understanding of the roles and responsibilities across policing for responding to fraud"*[152].

150. National Economic Crime Centre, 'Working together to protect the public, prosperity and the UK's reputation', accessed May 2020, link
151. Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services, 'Fraud: Time to choose - An inspection of the police response to fraud', April 2019, link
152. Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS), 'Fraud: Time to choose - An inspection of the police response to fraud', April 2019, link

Streamlining reporting of COVID-19 related public sector fraud

It is widely acknowledged that there are a number of challenges with the way that the UK central reporting hub 'Action Fraud' (National Fraud and Cyber Crime Reporting Centre - 0300 123 2040) currently works. These can be summarised as:

i. widespread confusion by the public about the role of 'Action Fraud' and where to report fraud;
ii. lack of capacity to manage fraud related calls even prior to the COVID-19 crisis;
iii. a lack of clarity about signposting victims and
iv. poor victim handling.[153]

The City of London police has historically had 'lead force' responsibility (and additional funding from the Home Office) for fraud investigation, a model that was established in a pre digital era when there was a need for a specialist capability to tackle large-scale corporate frauds emanating from the City of London financial centre. The City of London is responsible for national fraud policing strategy, investigating nationally significant, serious and complex fraud and leadership and coordination of victim care. It reports to the Fraud and Cyber Crime (National Systems) Board (chaired by the Home Office) that reports to the Economic Crime Strategic Board.

This 'lead force' City of London model has not, however, evolved as frauds have become digitalised, cyber enabled and prolific affecting the entire population. As a result, fraud investigation across the other 42 UK Police Forces is now poorly responded to. Many UK police forces don't investigate the packages that are sent to them by the National Financial Intelligence Bureau (NFIB) that works alongside Action Fraud, leading to frauds not being reflected in the local crime figures and hidden from reporting and accountability mechanisms. Local cyber-crime / fraud victims are also not given the same level of attention as other victims of traditional crime types.

It is widely acknowledged too that the Action Fraud reporting centre has too much demand which leads to victims receiving a poor service and becoming dissatisfied. The very title 'Action Fraud' doesn't deliver what it suggests. The concept of national reporting is a good one, but history, legacy and slow evolution has meant that opportunities to develop this model in a digitised world have not been acted upon quickly.

There are also three separate hotline numbers to report fraud to different parts of government. The National Fraud Hotline[154] (0800 854 440) deals with Housing and other benefit fraud (such as Universal Credit) on behalf of the Department for Work and Pensions whilst HMRC's Fraud Hotline[155] (0800 788 887) takes reports of all kinds of tax fraud and evasion including, for instance, PAYE and National Insurance Fraud, tax credit fraud, tax evasion and VAT fraud.

153. Police Foundation, 'More than just a number - improving the police response to fraud', December 2018, link
154. GOV.UK,'Report Benefit Fraud', link
155. GOV.UK, 'HMRC launches new Fraud Hotline', April 2017, link

The NHS Counter Fraud Authority also publicises an anonymous 24-hour fraud reporting line on 0800-028-4060 (powered by Crimestoppers).[156]

With the widespread increase of all forms of fraud related to the COVID-19 crisis, it is vitally important that the public have absolute clarity about how to report any form of COVID-19 related fraud, whether public or private. Consideration should therefore be given to creating a single **Fraud Hotline** for the public to report any aspect of fraud, waste, abuse or allegations of mismanagement involving the government's response to the COVID-19 crisis.

HMRC and the Home Office / NCA should also lead a COVID-19 economic crime / fraud public awareness campaign encouraging the public to report crime related to COVID-19 - specifically addressing the perception that fraud is victimless.

The Minister for Fraud and Economic Crime should oversee a programme of work that examines how the functions of 'Action Fraud' and the National Financial Intelligence Bureau (NFIB) can be merged in time into the National Economic Crime Centre (NECC) at the NCA leading to more effective reporting and monitoring of fraud allegations and the tasking of resources to investigate fraud. The City of London should retain its responsibilities to investigate nationally significant, serious and complex fraud but transfer its national responsibilities for oversight, reporting, monitoring etc. to the NECC.

156. NHS Counter Fraud Authority, 'Covid-19 related fraud prevention advice and guidance', May 2020, link

5. Using Technology To Prevent and Detect Public Sector Fraud

Introduction

The coronavirus crisis has exposed weaknesses in the UK's digital infrastructure that have allowed criminals to take advantage of the British government. As criminals develop new methods of exploiting technology to commit fraud, the UK public sector must develop and adopt more advanced methods to stop them. This applies particularly to crisis fraud. Technology is vital when it comes to fighting public sector fraud arising from the coronavirus crisis for two reasons:

- **Scale of crisis-related fraud:** the size and scale of recent Government interventions to support the economy during the public health crisis, as well as the high levels of participation in support schemes, are so great that post-pandemic efforts to identify fraud will struggle unless they are supported by technologies that enable investigators to operate at scale.
- **Exposure of existing weaknesses in digital infrastructure:** the implementation of social distancing measures has meant that public services which were previously delivered face-to-face have had to shift online. This shift highlighted a number of long-term weaknesses in the public sector's digital anti-fraud infrastructure (particularly in relation to identity assurance and digital identity). In addition, the need to develop online public services at pace may have increased the opportunities for fraud and error.

The adoption of anti-fraud technology is no replacement for skilled counter fraud investigation. The eradication of public sector fraud ultimately hinges on having the human resources available for investigation and the ability of prosecutors to bring cases forward. Nonetheless, this section explores how the Government can improve its use of anti-fraud technology by exploring:

1. How the public sector can make better use of data analytics and anti-fraud technology
2. COVID-19, digital ID and public sector identity assurance
3. Preventing fraudsters from impersonating the Government

1. How the public sector can make better use of data analytics and anti-fraud technology

Unless the UK Government makes use of the latest innovations in anti-fraud technologies, it is unlikely that it will be able to investigate fraud at the level and scale that the Coronavirus crisis requires. To quote the Government's own thought paper, *Tackling Fraud in Government with Data Analytics*, "historically Government's counter fraud responses have been reactive; focused on gathering intelligence and investigating low volumes of high value cases" which were "often identified through whistleblowing or random sampling."[157] In contrast, the scale of the Government's support schemes means that the Government will have to investigate high numbers of low to mid value cases, the volume of which could overwhelm investigators.

Preventing Fraud and Facilitating Investigations

The value of data analysis lies not simply in prompting or facilitating individual investigations. It also helps to prevent fraud from taking place by flagging fraudulent transactions in real time, spotting potential vulnerabilities and identifying the networks and Organised Crime Groups (OCGs) responsible for mass fraud. Indeed, data analysis techniques such as cluster analysis, outlier analysis, network analysis, machine learning, "fuzzy matching"[158] and others are regularly deployed in the private sector to detect fraud both in real time and after it has taken place.[159]

The use of document review technologies will be particularly important to fraud investigations post-pandemic. Indeed, the Serious Fraud Office (SFO) already deploys the use of AI-powered document review systems in its investigations, most notably during its investigations into Rolls-Royce bribery (a case which was settled for £671m).[160] According to the SFO, its AI-powered document review system saved the organisation 80 per cent of costs and time due to the fact that "the system was able to process more than half a million documents a day at speeds 2,000 times faster than a human lawyer".[161] Similarly, as part of the general grants transformation program, the 2020 budget launched a new £5 million programme to create digital tools to increase efficiencies and improve administration of general grants.[162] These tools (including anti-plagiarism software) should be used to improve the administration of COVID-19 Economic Support Schemes.

The application of Machine Learning for fraud detection has the capacity to transform the scale, speed and accuracy of COVID-related counter-fraud investigations. What makes Machine Learning systems particularly ideal for countering fraud, particularly when deployed in real time, is the fact that, if they have been designed optimally, they can earn, adapt, and uncover emerging patterns without over-adaptation and an excessive number of false positives. As the Alan Turing Institute rightly points out, "ML algorithms can analyse millions of data points to detect fraudulent transactions that would tend to go unnoticed by humans".[163]

157. Cabinet Office, DCMS, 'Tackling fraud in Government with data analytics', June 2019, link
158. "Fuzzy matching" refers to a technique where partial matches are used to link records together.
159. McKinsey and Company, 'Cracking down on fraud with data analytics', October 2018, link
160. BBC, 'Rolls-Royce apologises after £671m bribery settlement', January 2017, link
161. Publictechnology.net, 'Serious Fraud Office uses artificial intelligence to crack real crimes', June 2018, link
162. HM Treasury, Budget 2020, link
163. The Alan Turing Institute, 'Artificial intelligence in finance', April 2019, link

The Association of Certified Fraud Examiners (ACFE) in the US states that the use of AI for fraud detection will triple by 2021.[164] As the private sector increases in its use of Artificial Intelligence to detect fraud, so too will fraudsters start deploying the same technology to attack vulnerabilities.[165]This means that is essential for the public sector to keep up with the rate of innovation in the wider ecosystem. To do so, the UK must deploy both supervised and unsupervised ML systems to fight fraud.[166] The latter is particularly important because although rules-based approaches to ML are highly effective at detecting known fraud schemes, they're not as effective at adapting to new fraud patterns, uncovering unknown schemes, or identifying increasingly sophisticated fraud techniques.[167] Nonetheless, the use of unsupervised ML systems (particularly if deployed in real-time) must be subject to the highest ethical standards and the Government must ensure that there is sufficient transparency to enable public scrutiny of their use in so far as this is technologically possible.

Making Better Use of Cross-Government Data To Tackle Fraud

The use of data analytics to detect COVID-related public sector fraud is dependent upon ensuring that there is sufficient access to high-quality data. This applies particularly to the use of Artificial Intelligence. The availability of training data is arguably a greater determinant of the predictive accuracy of machine learning models than the type of algorithms they employ. Fraud models that are trained using data from a range of Government departments and agencies will be more accurate than models that rely on thin datasets.[168] Worryingly, a review by the Committee on Standards in Public Life into AI and Public Standards reported that, "Public policy experts frequently told this review that access to the right quantity of clean, good-quality data is limited, and that trial systems are not yet ready to be put into operation" and that "it is our impression that many public bodies are still focusing on early-stage digitalisation of services, rather than more ambitious AI projects."[169]

It is essential, therefore, that the COVID-19 Fraud Crime Hub has access to data from across Government to support its investigations. The Government recognises the importance of sharing data across Government when tackling fraud, which is why it rightly deploys a functional model in its approach to fraud through the Counter Fraud Expertise.[170] Indeed, improving the use of data fraud analytics was a priority for the Government before the scale of the public health crisis became apparent and it was announced in February that "a Government Counter Fraud Data Analytics Development project, led by Cabinet Office, will provide a counter fraud data analytics capability and run counter-fraud pilots across government, significantly reducing losses to the taxpayer through fraud."[171] The NCA's National Data Exploitation Capability has the capacity to help open up a wider range of public sector data assets. Although this capability has been developed to support investigations into all serious organised crime (SOC) and not just for fraud, it could be used to combine different sets of data from across the public sector to spot new networks and patterns.[172]

164. ACFE, *Press Release*, 'Study: AI for fraud detection to triple by 2021', June 2019, link
165. Future of Humanity Institute, University of Oxford, 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation', February 2018, link
166. During supervised ML, a set of "training data" that contains labels on the observations is supplied to the algorithm. The difference between supervised and unsupervised ML is that the latter lacks labelled training data and is left to determine correlations by itself.
167. Technology Review, 'Essentials for Fighting Fraud with Machine Learning, November 2019, link
168. Technology Review, 'Essentials for Fighting Fraud with Machine Learning, November 2019, link
169. The Committee on Standards in Public Life, 'Artificial Intelligence and Public Standards', February 2020, link
170. GOV.UK, 'The Functional Model: a model for more efficient and effective Government', link
171. The Cabinet Office, Letter to Meg Hillier MP, 'Re Challenges of Using Data Across Government', 10 April 2020, link
172. UK Authority, 'National Crime Agency aims to increase data capability', 20 March 2020, link

Counter Fraud Centre of Expertise and the National Fraud Initiative

- The Counter Fraud Centre of Expertise was founded in 2017 to provide fraud data analytics capability to the rest of government with the aim of supporting organisations to run data sharing pilots. This also includes the delivery of 14 pilots over the same period.
- The National Fraud Initiative (NFI) is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud.[173]

Although the Government has put in place the necessary legislation to enable public authorities to share data in order to prevent, detect, investigate and prosecute public sector fraudsters, more action is necessary. As Policy Exchange has pointed out consistently, Whitehall's departmental Structure intrinsically encourages a siloed approach to digital services and data storage.[174] As the Government itself made clear in section 14 of its COVID-19 Recovery Strategy (entitled "Sustainable Government Structures"), the epidemic has necessitated the "rapid re-engineering of government structures and institutions".[175] This applies particularly to the use of cross Governmental data. According to the National Audit Office, there are three issues hampering the use of data across Government:

- Data is not always seen as a priority;
- The quality of data is not well understood;
- There is a culture of tolerating and working around poor quality data.[176]

The Digital Economy Act (2017)

- Chapter 4 of Part 5 of the DEA enables the sharing of information between specified bodies to better combat fraud against the public sector.[177]
- The House of Commons Public Accounts Committee found that "there were 36 agreements under the new Act by July 2019, mostly aimed at reducing fraud and error and fuel poverty with slower progress in other areas."[178]

Improving the quality and availability of public sector data would do much to support innovation in the private sector.[179] For example, providing private sector companies (particularly those in financial services and FinTech) with access to registers such as those held by CIFAS, Companies House or the Land Registry in machine-readable formats would do much to prevent fraud outside the public sector.

It is essential to ensure adherence to common technical standards, data formats and definitions to ensure interoperability and to minimise barriers for anti-fraud related enquiries. Nonetheless, as the Public Accounts Committee Found, "leadership of initiatives to improve data is fragmented and unclear."[180] Indeed, the Government Committed itself to appointing a Chief Data Officer by 2020 but that and the newly-created

173. GOV.UK, 'National Fraud Initiative', 5 May 2020, link
174. Policy Exchange, *The Smart State*, May 2018, link; Policy Exchange, 'How to Transform The Government's Digital Leadership', January 2020, link
175. Cabinet Office, 'Our plan to rebuild: The UK Government's COVID-19 recovery strategy', 11 May 2020, link
176. NAO, Challenges in using data across government, June 2019, link
177. Digital Economy Act 2017, link
178. NAO, Challenges in using data across government, June 2019, link
179. Policy Exchange, *A Right to Data: Fulfilling the promise of open public data in the UK*, 2012, link
180. Public Accounts Committee, Challenges in using data across government, September 2019, link

position of Chief Digital and Innovation Officer (for which applications have had to be reopened once already) remained unfilled.[181] Moreover, whilst the Government Digital Service is responsible for data standards, the DCMS is responsible for data policy. Furthermore, the Government's *National Data Strategy* still hasn't been published, despite being announced in 2018.[182] Most worryingly, the Public Accounts Committee found that, "at July 2019, only 2 of 18 people attending the most recent meeting" of the Data Advisory Board (the senior oversight board across government) were permanent secretaries, despite these being the core members of the board.[183]

To improve the use of cross-Governmental data to tackle fraud:

- **The UK Government should explore the feasibility of creating a dedicated anti-fraud AI Lab.** Such a lab could accelerate the adoption of AI to tackle fraud across the public sector. Moreover, if it builds up sufficient data training sets, it would also be a suitable environment to train and test the efficacy of anti-fraud technologies.
- **2 identify public sector data assets that could support counter-fraud activities.** The strategy's aim is to "drive the collective vision that will support the UK to build a world-leading data economy".[184] Post-COVID, it should place a greater emphasis on monitoring the levels of fraud across both the public and private sector.
- **The Government should look to increase private sector participation in the National Fraud Initiative.** This will ensure that a greater range of private sector data is available to detect and fight fraud.
- **The Counter Fraud Centre of Expertise should run a number of COVID-specific data sharing pilots in conjunction with HMRC and other departments.** This will ensure that there is a wider range of data not just from the public sector but also the private sector to help detect and tackle public sector fraud.
- Encourage the NCA's National Data Exploitation Capability to combine different datasets from across Government Departments and Agencies to tackle public sector fraud.

2. Identity Assurance and Digital ID

The imposition of social distancing measures and the closure of government offices has meant that Government entitlements and benefits that were previously claimed, assessed or completed in-person or face-to-face have had to be completed online via the internet.[185] This poses a very particular problem for the UK Government: proving your identity online is very difficult in the UK. Digitising public services not only improves their access and availability but can also lead to economic efficiencies.[186] Nonetheless, unless people are able to prove that they are who they say they are online

181. Policy Exchange, 'How to Transform The Government's Digital Leadership', January 2020, link; Twitter, @rowlsmanthorpe, link
182. DCMS, National Data Strategy open call for evidence, June 2019, link
183. Public Accounts Committee, Challenges in using data across government, September 2019, link
184. DCMS, National Data Strategy open call for evidence, June 2019, link
185. This section aims to serve as a precursor to a wider report into digital ID and Identity Assurance that Policy Exchange are planning to publish later this year.
186. Alan Greenway, Ben Terett, Mike Bracken, Tom Loosemore, 'Digital Transformation at Scale: Why the Strategy Is Delivery', 2018

(to a high level of assurance) there will always be a bottleneck on the development of digital public services. More pertinently, fraudsters will thrive unless the Government develops reliable and accessible mechanisms to prove your identity when accessing public services and supports the development of a fully functioning digital identity ecosystem in the private sector.[187]

What is a digital identity?

- A digital identity is a collection of data belonging to a claimed identity, usually verified by trusted parties, which can be used as a digital representation of a unique person or organisation.[188] The main role of a digital ID is authentication: to verify whether an entity is who (or what) they (or it) is believed to be and whether they are worthy of trust.
- The UK Government defines a digital identity as "a trusted way of proving one or more attributes about themselves online or offline and linking those attributes to that same person as a uniquely identifiable individual."[189]

Ensuring that online services are easily accessible to citizens whilst also ensuring that sufficient identity checks are completed in order to prevent fraudulent activity and unauthorised access to those services has been a complex challenge for Governments and businesses in the UK and abroad.[190] Industries, such as banking, which traditionally relied upon physical IDs to authenticate customers and employees have had to undergo a radical transformation to adapt to the conditions that COVID-19 has imposed on our lives to provide secure online services for their customers.[191]

The Coronavirus crisis highlighted the limitations of public sector identity assurance systems. There have been hugely impressive attempts to scale up the Government's main identity assurance platform, GOV.UK Verify.[192] Nonetheless, due to the Coronavirus Crisis, it was announced that it had to receive further public funding for an unexpected additional 18 months (despite the fact that its funding had already been extended once before and that the platform has cost over £175m already).[193] Moreover, HM Treasury has reportedly made these funds dependent upon the condition that the Government Digital Service does not add any further services to the Verify roster.[194] This development followed a troubled history: in 2019, both the National Audit Office and the Infrastructure and Projects Authority recommended that the Government terminate the project.[195]

Why Public Sector Identity Assurance is Necessary

COVID-19 related identity fraud will be aided by the growing online marketplace for identity documents on the dark web. Stolen personal identifiable information (PII) can be obtained from cyber attacks.[196] This can allow fraudsters to invent synthetic identities, in which a criminal combines real and fake information to create a new identity, or to take over

187. TechUK, *Digital Identity White Paper*, February 2019, link
188. OIX, Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK: White Paper, October 2019, link
189. DCMS and Cabinet Office, *Digital Identity: Call for Evidence*, July 2019, link
190. TechUK Event, *Now More than Ever*, 21 May 2020, link
191. Planet FinTech, *'Digital Identity Verification 'on the rise' amid Coronavirus'*, link
192. GDS, Cabinet Office "Scaling up GOV.UK Verify to help during coronavirus", 11 May 2020, link
193. Parliament.UK, Digital Identity and GOV.UK Verify Programme Update:Written statement - HCWS217, link
194. ComputerWeekly, 'HM Treasury tells GDS: No further online services can use GOV.UK Verify', 7 May 2020, link
195. NAO, 'Investigation Into Verify', March 2019, link; UK Authority, 'Government auditor blasts GOV.UK Verify', 5 March 2019, link
196. Fraud Magazine, April 2014, link, HBS Digital Initiative, 'The Growing Market for Identifying Fake IDs', 13 November 2018, link

real identities to commit fraud and to take advantage of the Government's COVID support schemes.[197] This means that it is essential for public sector organisations not just to check that information that users submit when trying to access services relates to a real person but why it is also essential to obtain proof of genuine presence assurance to determine that they are the person they are claiming to be.[198] The latter is especially difficult to do over the internet and is often achieved by checking user biometric data, for example, thumbprints, DNA, face recognition, retina scanning. This makes it potentially controversial from a civil liberties perspective.[199]

Types of Identity Fraud

True (Traditional) Identity Fraud: this is the simplest type of fraud and implies the stealing or purchasing of a victim's identity details (or credit card or payment details) on the Dark Web.

Synthetic Identity Fraud. There is a growing online marketplace for identity documents on the dark web. Stolen personal identifiable information (PII) can be obtained from cyber attacks.[200] This can allow fraudsters to invent synthetic identities, in which a criminal combines real and fake information to create a new identity, or to take over real identities to commit fraud.[201] There are two methods used by fraudsters to create synthetic identities:

- **Manipulated Synthetics** are based on a real identity and only limited changes are made to the identity, usually to hide previous history.[202]
- **Manufactured Synthetics:** are composed of valid data assembled from multiple identities. They are often referred to as 'Frankenstein' identities because fraudsters cobble together bits and pieces of personally identifiable information (PII) from real people to create fake identities.[203]

How Technology can be used to detect identity fraud

The greater the level of checks that are completed on an identity assertion, the higher the level of assurance that the Government has in that assertion and the less chance there is of fraud being committed.[204] Identity document validation technologies (IDVT) provide the foundations for standards-based digital ID ecosystem. There are three main purposes to these technologies:

- **Authentication:** They confirm that the documents provided by a customer are not forged and that they are authentic.
- **Validation:** They confirm that an identity document hasn't been stolen or that it hasn't expired.
- **User Assurance:** They confirm that an identity document relates to the holder and that the person trying to access services isn't using documentation relating to others.[205]

197. ID Crowd, 'Why we need standards based digital identity', 19 November 2018, link
198. Iproov.com, 'Genuine Presence: The three tiers of security', 12 December 2019, link
199. Yoti, 'Digital Identity Explained', link
200. Fraud Magazine, April 2014, link, HBS Digital Initiative, 'The Growing Market for Identifying Fake IDs', 13 November 2018, link
201. ID Crowd, 'Why we need standards based digital identity', 19 November 2018, link
202. Idanalytics.com 'What is Synthetic Identity Fraud?', link
203. Idanalytics.com 'What is Synthetic Identity Fraud?', link
204. Cabinet Office, Government Digital Service, 'Good Practice Guide (GPG) 45', 19 March 2020, link
205. Home Office, 'Identification Document Validation Technology', 28 March 2018, link

IDVTs usually consist of the following technologies (many of which are contained in the hardware of an average smartphone):

- **Scanning Devices:** to scan an identity document or take a photograph to sufficiently high standard.
- **Optical character recognition (OCR) software:** such software converts images of the text on an identity document into machine-encoded text, which allow the details it contains to be checked against records.
- **Templates library of identity documents:** these templates can be used to check the security features on submitted identity documents and compare its contents against templates stored in the library to determine whether the identity document is authentic.
- **Access to other datasets:** IDVTs must be able to make checks against other databases, such as Interpol's lost and stolen passport data, to ensure that identity documents are valid. This is done in the UK by the document checking service.[206]

How COVID-19 Affected The UK Government's Different Identity Assurance Platforms

The COVID-19 crisis has forced the Government to adapt its identity assurance standards. As the NAO has already highlighted, "to get support to those that need it quickly, departments have had to relax the controls and checks they would normally have in place to administer and deliver schemes of support" thereby increasing "the risk of fraud and error."[207] Indeed, the longer and more rigorous the process of checking identities, the greater the friction for users accessing public services. It is unsurprising, therefore, that the NAO estimate that the Government has had to spend an additional £28m on support for Government digital services, including "to support systems that help Universal Credit claimants verify their identity and a new service to track 1.5 million vulnerable people".[208]

The UK differs from many European countries because it lacks a Government-mandated and centrally supported biometric ID card. Such cards often provide the basis of national digital ID schemes and can be used by citizens to access online services provided by both the public and the private sectors.[209] The UK Government has a long-standing political commitment not to introduce biometric identity cards or establish a central database of citizen attributes following the repeal of the Identity Card Act (a decision taken in part on civil liberties grounds).[210]

The UK Government has a number of different identity assurance systems that departments use to verify the identities of citizens accessing their services**.** The two main ones are:

- **GOV.UK Verify:** GOV.UK Verify allows citizens to prove their identities online when accessing Government Services. It operates without a central government database of citizen attributes and works with certified companies, known as identity providers

206. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
207. National Audit Office, 'Overview of the UK Government's Response to the COVID 19 pandemic', May 2020, link
208. National Audit Office, 'Overview of the UK Government's Response to the COVID 19 pandemic', May 2020, link
209. E-estonia, 'e-identity', link
210. Identity Card Act 2006 (Repealed), link

(IDPs), to prove users' identities.[211] In order to create a Verify account you have to provide some personal information which is then checked against a variety of different records. Once these have been checked, you can use Verify to access Government services online such as the receipt of benefits or to pay tax bills. GOV.UK Verify was designed with the intention of preserving user privacy.[212]

- **HMRC Government Gateway:** The pan-government Government Gateway Transformation Programme (GGTP) is an HMRC programme and is key to the government's digital transformation agenda.[213] GGTP provides access to over 120 government services, provides credential management, hosts relevant databases and manages defined bulk data transfers of data between government and organisations.[214] At its core, "Gateway" is a system for creating a user ID and password for use with Government services. Since its creation HMRC have added support for 2nd Factor Authentication. HMRC data is used to ask verification questions and to create an ID you need to create a passport number.

The COVID-19 crisis exposed the weakness of these systems. Although the Document Checking Service is an incredibly valuable asset to the UK Government, as noted above, the Government was supposed to stop funding the GOV.UK Verify system (which has cost over £175m already) in April 2020.[215] Due to the surge in numbers of people claiming Universal Credit, HM Treasury agreed to provide it with public funds for a further 18 months reportedly on the condition that GDS did not add any further Government services to the Verify roster and that the GDS create alternative identity verification tools for services solely reliant on Verify.[216]

Document Checking Service

- The Document Checking Service checks passport details against the HM Passport Office (HMPO) database. It provides a simple 'yes' or 'no' response to say whether a passport is valid without giving direct access to government-held data.[217]
- It is a huge economic asset to the Government due to the fact that it could transform identity assurance in the private sector (particularly in the financial service and FinTech Sectors) by allowing private sector organisations to use it to check the identities of their customers.
- The Document Checking Service Pilot allows the non-public sector organisations participating to pay to access the service to find out if British passports are valid.

At the start of the Coronavirus (COVID-19) Crisis, the Department of Work and Pensions connected to HMRC Government Gateway to provide additional support for Universal Credit applicants in addition to GOV.UK Verify.[218] Whereas GOV.UK Verify was primarily set up to determine

211. Government Digital Service, 'GOV.UK Verify', accessed 11 June 2020, link
212. Government Digital Service, 'GOV.UK Verify', accessed 11 June 2020, link
213. HMRC, 'HMRC Government Gateway Transformation Programme: : Accounting Officer assessment summary', 18 March 2019, link
214. HMRC, HMRC Government Gateway Transformation Programme: : Accounting Officer assessment summary, 18 March 2019, link
215. Civil Service World, 'Government to hand GOV.UK Verify over to private sector and cease funding', 10 October 2018, link
216. ComputerWeekly, 'HM Treasury tells GDS: No further online services can use GOV.UK Verify', 7 May 2020, link
217. DCMS, GDS, 'Apply for the Document Checking Service', 1 May 2020, link
218. Computer Weekly, 'DWP turns to Government Gateway to support Universal Credit claims', 16 Apr 2020, link

whether somebody should be entitled to receive payments, HMRC's system has developed to make the payment of tax more simple and secure. As a result, while HMRC's Government Gateway service includes 2nd Factor Authentication and while you do need to submit passport data, there may be fewer checks to guarantee that the passport you are submitting belongs to you even if it is a legitimate document. While this may streamline processes and make it easier for people to pay their tax, this nonetheless may result in a lower level of identity assurance for those transactions.

The Limitations to GOV.UK Verify

- GOV.UK Verify has missed its targets. It has not signed up 25 million users by 2020, as was predicted. All but two of the certified companies acting as identity providers dropped out of the scheme. In 2019, both the National Audit Office and the Infrastructure and Projects Authority recommended that the Government terminate the project.
- GOV.UK Verify was a creative solution to the UK Government's desire to receive identity assurance without the use of biometric ID cards and central citizen attribute registries. It has struggled because it was launched before other Government Departments had promised to participate in the scheme. Moreover, its 'closed' commercial framework limited the number of companies who could act as certified companies and provide identity assurance to the Government. The UK Government also missed key opportunities to sign up people to the scheme when they were completing identity checks on their citizens. Crucially, the service struggled to balance ease of access (ensuring that users managed to verify their identity in a frictionless way) with the necessary and important tests that are required to prevent fraud, resulting in a poor user experience. Crucially, the Government was unable to make sufficient use of Government data sources in the identity proofing and verification process, making it more difficult for certain demographics with weak digital footprints (known as "thin file" users) to sign up.

To improve the UK's Digital ID infrastructure:

- **The Government should extend the scope of the Document Checking Service and increase participation in the DCS Pilot Scheme.** The Document Checking Service Pilot Scheme should be extended and the number of private sector participants expanded. At present, it is only possible to check passport data against HM Passport Office data. The service should be extended to check other identity documents.
- **Use Government data resources to improve identity proofing and verification processes.** The more resources that Departments can use to verify people's identities, the more likely they are to detect fraudsters and 'pass through' identity checks without encountering unnecessary friction. The Government should evaluate data resources that could be used to to help verify identity

assertions.

- **The Government should accelerate the creation of *Confirm My Identity*.** The Government should also provide clarity on the future of GOV.UK Verify. The creation of a tailor-made identity solution for the DWP should be encouraged because those reliant on welfare are more likely to lack the necessary ID documents, as Policy Exchange highlighted in *FinTech For All*.[219] Nonetheless, there are clear advantages to developing cross-departmental identity solutions and there is a risk that every department will develop siloed approaches to identity assurance, leading to increased costs for Government and hampering the potential of digital IDs to transform public services and give citizens control of their own data.
- **Introduce more rigorous identity checks for Companies House directors.** Although Companies House is currently undergoing significant reform, introducing rigorous checks on Companies House directors would help to prevent fraud in the future.[220]

3. Impersonating the Government online

Although not technically fraud against the public sector, there have been significant efforts to tackle COVID related cyber-crime. The National Cyber Security Centre launched the Suspicious Email Reporting Service, which was co-developed alongside the City of London Police. This allows law enforcement to pull live-time analysis of reports from the public, which can help them identify new scams and new patterns in online offending quicker than was previously possible. It has been incredibly popular; the UK public has flagged over 160,000 suspicious emails to new service in just two weeks.[221]

Domain-based Message Authentication, Reporting and Conformance

DMARC verification is an email protocol being adopted globally. It verifies that the purported domain of the sender has not been impersonated.

One of the key ways to detect an email phishing scam is to determine whether the email address matches the institution the email claims to represent. Domain spoofing can enhance traditional email phishing techniques by making it appear that the email is from a Government body or respected institution.[222] 80 per cent of banks accredited for the Coronavirus Business Interruption Loan Scheme (CBILS) have not implemented the strictest level of DMARC (Domain-based Message Authentication, Reporting & Conformance) protection – an email authentication protocol that verifies that the purported domain of the sender has not been impersonated.[223] Almost two thirds of accredited banks have published no DMARC record at all, leaving the doors to impersonation attacks flung open, according to Proofpoint.[224] This represents a wider problem for public institutions. In

219. Policy Exchange, 'FinTech For All', 14 January 2020, link
220. BEIS, Companies House, 'Consultation, Corporate transparency and register reform', link
221. NCSC, Press Release, 'NCSC shines light on scams being foiled via pioneering new reporting service', 7 May 2020, link
222. IAS Insider, 'Four Types of Domain Spoofing', link
223. Proofpoint, Press Release, link
224. NewStatesman, 'UK banks exposing businesses to risk of Covid-19 email fraud, says Proofpoint', 12 May 2020, link

2019, almost two thirds (65 per cent) of the UK's top 20 Universities have no published DMARC (Domain-based Message Authentication, Reporting & Conformance) record, making them potentially more susceptible to cybercriminals spoofing their identity and increasing the risk of email fraud for students.[225]

To prevent fraud predicated upon the impersonation of the Government and institutions with access to public funds, the UK Government should:

- **Require all banks accredited in the Coronavirus Business Interruption Loan Scheme and NHS Trusts to introduce the highest email authentication protocols**. The UK Government should also work with industry bodies to promote the use of email authentication protocols in the wider private, educational and charitable sectors.
- **Further advertise the existence of the Suspicious Email Service.** After the service was promoted on the Martin Lewis Money Show, there was an increase of over 10,000 additional reports in just one day. The UK Government has already announced its plans to support the journalism industry through the "All in, all together" newspaper advertising campaign.[226] The promotion of the Suspicious Email Service should be part of this advertising campaign.

225. Proofpoint, Press Release, 'UK Students at Risk of Email Fraud Ahead of A-Level Results Day', August 2019, link
226. NCSC, Press Release, NCSC shines light on scams being foiled via pioneering new reporting service, 7 May 2020, link

Conclusion

Public sector fraud is a problem that has been ailing the state long before coronavirus infected the country. While significant improvements have been made over the last decade in terms of the detection and prevention of fraud, there is still a long road ahead, with many of the opportunities for fraudsters difficult to anticipate.

While a sharp increase in the amount of fraud committed against the British government has been an unintended consequence of the Government's interventions to prevent the spread of the disease and the destruction of the economy, we should not become accustomed to this level of fraud. Despite the fact that many commentators describe it as a 'necessary evil', we should not allow this to reduce the zeal with which we continue to tackle it. The persistent fight against fraud is vital to maintaining confidence in the State and restoring the faith of British taxpayers in the belief that its Government can protect the public purse.

Appendix 1

We have calculated predicted Government expenditure as a result of the COVID-19 crisis by combining data provided in the OBR *Coronavirus policy monitoring database - 19 June* 2020 with data released by the Treasury along with Rishi Sunak's Economic Update on the 8th July 2020. Where appropriate, we have applied a 0.5 per cent - 5 per cent rate of fraud, which is the standard measurement used by the Cabinet Office to predict the scale of public sector fraud in the UK.[227] For welfare spending, we use a higher rate of 7.6 per cent fraud, as the increase in welfare spending is primarily on Universal Credit, which has this higher rate of fraud according to the Department for Work and Pensions.[228] For a full breakdown of the £154.3 billion expected expenditure and varying fraud rates, see Table 1.

Table 1: Breakdown of estimated cost of Government interventions as a result of COVID-19 crisis and the accompanying fraud rates.[229]

	Cost (£bn)	Fraud Rate	Lower Bound (£bn)	Upper Bound (£bn)
DEL measures				
Public service spending, funding for charities, culture and vulnerable people	51.1	0.5 per cent to 5 per cent	0.2555	2.555
Employment support				
Coronavirus job retention scheme	60	0.5 per cent to 5 per cent	0.3	3
Self-employed income support scheme	15	0.5 per cent to 5 per cent	0.075	0.75
Other support for households				
Statutory sick pay support	0.2	0.5 per cent to 5 per cent	0.001	0.01
Welfare package	8	7.60 per cent	0.608	0.608
Business support: tax and spending measures				
Small business grant schemes	15	0.5 per cent to 5 per cent	0.075	0.75
Business support: loans and guarantees				
Loan schemes (CBILS, CLBILS, BBLS)	5	0.5 per cent to 5 per cent	0.025	0.25
Total	154.3		1.340	7.923

227. Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', 2020, Link

228. Department for Work and Pensions, 'Fraud and Error in the Benefit System 2019/20', link

229. OBR, *Coronavirus policy monitoring database - 19 June 2020*, link; HM Treasury, 'A Plan for Jobs 2020', *GOV.UK* [website], July 2020, link; Cabinet Office. 'Cross-Government Fraud Landscape Annual Report 2019', 2020, Link; Department for Work and Pensions, 'Fraud and Error in the Benefit System 2019/20', link; Martin Arnold, 'Furlough fraud plagues Europe's drive to save jobs from pandemic', Financial Times, May 2020, link.

It is worth noting that this estimate does not include the up to £30 billion worth of additional spending announced in the Economic Update on the 8th July 2020. There is insufficient information as to the delivery of these schemes to include accurate fraud estimates, as well as a lack of information regarding the expected uptake of the Job Retention Bonus, which could constitute up to a third of this additional spending.

Furthermore, this estimate includes only the expected fraud rate on government expenditure for a small number of defaulting loans, as the OBR estimates a 10 per cent default rate across business support loans and guarantees. This is much lower than the default rates expected by many banks, who for example predict that between 40 per cent and 50 per cent of BBLs may default. Therefore it is likely that the government expenditure on the loan schemes will be greater than 10 per cent of the total loans, which will result in a larger amount lost to fraud than in these estimates.

Similarly, changes made to Universal Credit over the course of the coronavirus crisis has made fraud easier and more attractive. We can therefore expect the amount lost to welfare fraud to be higher than in this estimate. On the other hand, our estimate does not take into account the impact of part-time furlough onto the total cost of furlough, which may reduce overall expenditure on furlough payments for the final three months of this scheme. It is also worth noting that as highlighted in Chapter 2, studies from the Johannes Kepler University demonstrate that equivalent European schemes to the CJRS may experience fraud rates of 8 per cent - 10 per cent. If the CJRS suffers from this rate of fraud, which is not unlikely, the Government will lose an additional £3.2 billion to fraud.[230]

Furthermore, it is difficult to extrapolate an estimate of fraud in a linear fashion. Although the increase in government spending and relaxing of procedures and due diligence may attract more fraudsters, they may not be able to scale up their operations to take on the increase in public expenditure at the same rate they are used to. Additionally, an increase in coronavirus fraud may result in lower levels of public sector fraud in other areas. Despite these difficulties, we believe it is important to produce an estimate, as conducting post event assurance will be resource intensive, so it will be vital that the government and the public realise what is at stake.

230. Martin Arnold, 'Furlough fraud plagues Europe's drive to save jobs from pandemic', Financial Times, May 2020, link

£10.00
ISBN: 978-1-913459-33-8

Policy Exchange
8 – 10 Great George Street
Westminster
London SW1P 3AE

www.policyexchange.org.uk