Fraud, Pandemics and Policing Responses

Michael Levi
School of Social Sciences, University of Cardiff

Abstract
The article identifies some novel crime types and methodologies arising during the current pandemic that were not seen in previous pandemics. These changes may result from public health measures taken in response to COVID-19, the current state of technologies and the activities of law enforcement and regulators. It shows that most frauds that we know about might have occurred anyway, but some specific – mainly online - frauds occur during pandemics, and because of large scale government assistance programmes to businesses and individuals, many more opportunities were created from Covid-19. In the UK and Australia (less clearly elsewhere), public-private partnerships between police and banks led to joint activities in the attempted prevention of public-facing frauds (though the success measures are unclear), and arrests of suspects were sometimes easier because they were at home more! However, responses to fraud against government loans and grants were weaker and it is likely that many of them will be unprosecuted. More frauds will come to light later. More rapid prevention is the key to reducing the impact of economic crimes, but we need better focused research on how to get people not to fall for scams, better technologies to make frauds harder, and better processes and political will to stop procurement frauds.

Keywords: Corruption, Covid-19, cybercrime, economic crime, fraud, pandemics, policing, prevention.

Introduction

It is too easy to assume that COVID-19 has led to more frauds. We must consider the full range of deceptions, some of which – like dubious or counterfeit products promoted by businesses and celebrity 'influencers' – have a larger market during pandemics; others (like romance frauds) are more effective during times of isolation; and others still like pandemic government grants and loans are created to cope with the pandemic. We need also to consider the attractiveness and ease with which organised crime and professional fraud networks can increase the supply of these frauds. What lessons have been learned, or not learned, from previous crises, and what can we plausibly learn from Covid-19? How likely are we to actually put these lessons into practice? Perhaps the answer depends on you, the readers!

Fraud or economic crime is the Cinderella area of policing. Most frauds are undetected or detected but unreported and unrecorded. This can vary from country to country and over time, but though its precise dimensions are unknowable or contestable, household

and business crime surveys can and in some European countries do measure some dimensions of it (Levi & Burrows, 2008; Levi, 2017; ONS, 2020). The elapsed time from a fraud beginning to its formal detection and successful bringing to justice can take many years or even never happen at all. Large internal frauds and corruption usually take longer to appear and also to investigate and prosecute than volume frauds like payment card frauds and romance scams. So we need to be aware that what we see in front of us only tells part of the story.

Changes in monitoring and policing or regulatory responses might be responsible for changes in official data, so we cannot assume that changes in reported or recorded 'fraud rates' are real reflections of underlying frauds. Likewise, the pandemic alters the shape of official responses. On the one hand, there may be less police investigation due to constraints on transport and face-to-face working: but some law enforcement agencies (e.g. the City of London police) have used the opportunity to make arrests, which have become more efficient since many suspects are at home during lockdown. The hacking (initially by the French) of encrypted criminal communications like Encrochat [1]or the planting (mainly by Australians and Americans) of pseudo-encrypted apps like ANOM might had more impact on fraud and other economic crimes if the hardware and software had been distributed beyond drug trafficking networks[2]. But these technological breakthroughs coincided with the pandemic - they were not caused by it. There also remain some contestable issues within and outside the EU: when do homeopathic and prescription 'cures' for which there is no good scientific evidence become 'criminal deceptions' under separate national legislation? Finally, the article reviews what can be learned from law enforcement and other responses to economic crimes during the Covid-19 pandemic.

Fraud during the coronavirus pandemic

The patterns and levels of fraud should be seen against the backdrop of the general economy and patterns of economic and social life. We know that many people find it difficult to distinguish between real and nominal interest rates, but when nominal interest rates are very low as they have been just before and during COVID-times, offers of higher returns from markets (including cryptocurrencies) become even more attractive, especially when fake reassurances are given about what the funds will be invested in and whether the firm is authorised.

The shift towards the use of online platforms and teleworking during the 2019-21 pandemic has underlined the opportunities to offenders (including 'undermining' opportunities) as well as to business and Working from Home provided by digital technologies. As was already the case before, access to such opportunities has varied substantially within and across countries. Eurostat data show large EU MS variations in rates of online access and e-commerce.[3] The rise in ransomware attacks has also generated more political, law enforcement and corporate concern, though their connection with the pandemic is only occasional, via Phishing or Business Email Compromise to freeze and lock up business IT systems, which has been growing fast during home working. Worldwide corporate spending on online security is expected to hit $150bn in 2021, compared with $113bn in 2018:[4] but data on the specific European dimensions of this are unavailable.[5]

Quantification of the scale is hampered by a number of factors. First there is the problem of what we count and in what area. ENISA has focussed on costs to SMEs and to Critical National Infrastructure, and so too will the new Joint Cyber Unit, established by the European Commission. In my judgment, a much broader range of and set of sources for economic crime data against individuals, business and government is available from the UK, the Netherlands and Sweden than elsewhere, but there is the problem of determining the causal relationship between the pandemic and those frauds that

1 https://www.computerweekly.com/news/252499785/French-legal-challenge-over-EncroChat-cryptophone-hack-could-hit-UK-prosecutions; https://www.thetimes.co.uk/article/the-encrochat-bust-how-police-hacked-the-secret-gangster-messaging-network-mjvh3xlxw.

2 Some network members would have been involved in economic crimes, and perhaps all in money laundering because all major crime groups require at least some proceeds to be laundered.

3 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

4 https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

5 For a broader discussion of crime risks and threats, see Europol, 2021; and for a recent popular analysis, Reitano & Shaw, 2021. For early analyses of cybercrimes, see Buil-Gil et al., 2020; Vu et al., 2020; and Horgan et al., 2020.)

are detected during or after it. The disruption caused to business operations often simply results in existing frauds being uncovered, so we need to look at when those frauds happened. During the pandemic, many companies that normally would have failed were artificially supported by government payments, resulting in numbers entering external administration declining. Once government support payments decline or end, we can expect that these numbers will increase considerably, but much depends on the staffing resources, competence and incentives to follow things up and classify them as 'crimes'. Even before the pandemic, concern was expressed in the United Kingdom about the potential abuse of pre-pack administration to enable directors (in their own names or in those of nominees) to repurchase the assets from their businesses cheaply and walk away from their corporate debts, rising again like a phoenix from the flames (Levi, 2008).

Typologies of fraud during the coronavirus pandemic

Consumer scams

As the coronavirus pandemic spread from 2019 and into 2021, social distancing measures required most working and non-working people to remain in their homes, leading to intense reliance on digital technologies to work, to save/invest/transfer funds and to communicate with families and friends outside their homes. This created substantial opportunities for individuals to commit online fraud and to be victimised on a widespread scale (Europol, 2020, 2021; Walker, 2020). Cybersecurity problems have also arisen due to home-based workers not adhering adequately to business cybersecurity policies, such as user authentication protocols, as well as improper sharing of sensitive corporate data with unauthorised family members and others.

As time went on, ongoing working from home and social restrictions led to a boom in pet ownership.[6] This stimulated a wave of frauds about the breeding histories of animals, and scams on those who had lost pets or had them stolen and advertised for their return. The UK National Cyber Security Centre (NCSC, 2020) has noted phishing and malware related to health advice, contact tracing, funds and rebates, and fake goods and services—from PPE to disinfecting driveways.

Bereavement scammers have targeted families organising funerals by purporting to be from their local authority's bereavement services team and asking for credit card details to pay the funeral director. Families are told that the funeral will be cancelled if they do not pay immediately. Some e-commerce sites that arose in 2020 offered a range of extraordinary products for sale (see Keller & Lorenz, 2020).

Consumer protection organisations across the globe began receiving complaints and notifications from victims of these scams, with substantial losses being suffered. In the UK, as early as 6 March 2020, the National Fraud Intelligence Bureau reported at least 21 confirmed cases of coronavirus-related fraud, with victims losing more than £800,000. Half of these reports were made by victims who tried to purchase large orders of surgical masks from fraudulent merchants who took their money but did not deliver product of the right quality. The others included victims of various fake website phishing attacks. In March 2020, Operation Pangea XIII was conducted by police, customs and health regulators from 90 countries, all aiming to prevent illicit online sales of medicines and medical products. Counterfeit face masks and unauthorised antiviral medications were all seized under the operation. Counterfeit medicines and vaccinations were sometimes investigated in collaboration with Europol[7] In 2020, the NCSC (2020) scanned more than 1.4m National Health Service IP endpoint addresses for vulnerabilities, leading to the detection of 51,000 indicators of compromise. It also worked with international allies in the Global North to raise awareness of the threat to vaccine research, particularly from Russian cyber actors with intelligence service connections (NCSC, 2020, p.20).

The range of adaptations of conventional scams to the pandemic environment has been extensive, with criminals developing scams involving PPE and fake cures, domestic pet scams, employment scams, investment frauds, travel refund and insurance scams, and a variety of phishing attacks, identity crimes and ransomware threats involving COVID-19 scenarios, sometimes impersonating contact tracing officials to obtain personal and banking information. There have also been reports of false charity scams and phishing emails claiming to provide important information regarding the latest

6 e.g. https://www.pfma.org.uk/news/pfma-confirms-dramatic-rise-in-pet-acquisition-among-millennials.

7 see https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know; https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic

coronavirus updates, local testing stations, potential cures, cheap medical products or working from home. In addition to attempts by airlines themselves to disincentivise air ticket repayments, there have also been reports of ticket refund fraud due to travel restrictions, romance fraud, charity fraud and financial loan fraud (Action Fraud, 2020). Online loan sharking now has a higher success rate as unemployment and the global economic downturn caused by the pandemic has left many indebted and impoverished (Felbab-Brown, 2020).

Some COVID-19-related frauds have involved pure cyber-dependent activities. Many coronavirus-related domains have also been registered by cybercriminals, leading officials to warn users to not open attachments or click on links in emails coming from so-called informational websites. For example, a Twitter user, @dustyfresh, published a web tracker that found 3,600 coronavirus and COVID-19-related hostnames created in the preceding 24 hours (Ruiz, 2020). RiskIQ (2020), a US-based cybersecurity company, tracked more than 13,000 suspicious coronavirus-related domains over a weekend, with more than 35,000 new domains discovered the following day. Technology has also facilitated the sale of medical supplies and PPE during the coronavirus pandemic. A caveat is in order: data on fake availability tell us little about market size of fakes as a *proportion* of products purchased. The UK NCSC has identified CEO-simulating requests for remote staff to purchase Google Play cards and Microsoft-simulating requests to change office VPNs: these *could* have occurred before the pandemic, but were more credible to staff during it. It is not known how many people fell for this scam and what the impacts were. Business email compromise scams have become common throughout Europe.

Many Romance scams used Covid-19 as a rationale, but most fraud cases had nothing directly to do with the pandemic directly, though vulnerability might be increased by physical isolation from family and friends. In the year to April 2021, the City of London police stated that 5,039 investment fraud reports involving over £63m losses nationally referred to a social media platform as part of the medium for the scam, with 44.7 per cent of reports stating the fake commodity they had been scammed into investing in was a type of cryptocurrency. In the reports, Instagram was the most referenced platform (35.2 per cent), followed by Facebook (18.4 per cent). The national fraud reporting body Action Fraud received over 500 investment fraud reports which made reference to a bogus celebrity endorsement, with losses reaching over £10m in 2020-21.[8]

The national reporting system for phishing emails which began April 2020 was used heavily and in a sustained way.[9] Though the longer-term prevention and deterrent effects of the 'whack-a-mole' approach are as yet unknown, as of 31 May 2021, the number of reports received by NCSC in just over a year stand at more than 6,100,000, and over 45,000 scams and 90,000 URLs were removed, including over 300,000 malicious URLs linking to faked celebrity-endorsed investment schemes which are not specifically linked to the pandemic.

The extent to which these are 'excess scams' (by analogy with 'excess deaths') is hard to identify, especially at this early stage. However, they demonstrate the rapidity with which at least some criminals are able to adapt the narratives on which to hang their deceptions. They also show the imperfect (and largely unresearched) impact that regular warnings in the media and policing interventions have had in stopping victims from falling for them (for which assessment we need to know what the counterfactuals would be).

Payment card fraud

At the beginning of the Pandemic, there were predictions of a boom in frauds of various types. How did that work out? We need first to distinguish between short term and longer term frauds, with differential rates of visibility. First among these are payment card frauds. Unfortunately, the most recent card fraud statistics for SEPA published by the European Central Bank are for 2018 (ECB, 2020), so they are not helpful at all for analysing the impact of Covid-19: they will not be until they are published in 2020 and 2023! We must therefore rely on private sector firms' data, of which the fullest and most recent are in the UK (UK Finance, 2021). In fact, the UK led in reducing card fraud losses in Europe[10], though its rate of card fraud per Euro spent is the highest, followed by France, Denmark, Sweden and Spain. Whilst Europe had a €62m reduction in payment card fraud losses for 2020, this was driven by the UK with a £46M (€69M) reduction and Denmark with a €20M reduction, mostly in card-not-present fraud. Only 5 of the 18 countries contained with-

8 https://www.cityoflondon.police.uk/news/city-of-london/news/2021/may/new-figures-reveal-victims-lost-over-63m-to-investment-fraud-scams-on-social-media/

9 Author interviews.

10 https://www.fico.com/europeanfraud/

in the FICO study had card fraud reduced. At the other end of the scale, Norway posted the largest increase. France, Poland and Germany showed ongoing increases in losses, but these were not large figures in relation to the volume of business. Turkey, Spain and the Czech Republic all showed a relatively flat trend through 2020.

Throughout 2020, social engineering has been used to make use of the global pandemic to trick unsuspecting users into providing funds or information to criminals. However, the COVID-19 pandemic has led to a fall in contactless card and cheque fraud in 2020 as the lockdown restrictions reduced opportunities for criminals to commit these types of scams. Cases of fraud on lost and stolen cards have also fallen significantly due to the restrictions in movement as a result of the pandemic, though push payment scams in which criminals trick their victims into sending money directly from their account to an account which the criminal controls have increased (UK Finance 2021, pp. 12, 20). Whilst losses have been decreasing, the number of confirmed cases – accounts, not individuals - has increased during 2020, rising by four per cent to 2,835,622 cases after a five per cent rise the previous year. This demonstrates that cases are being spotted and stopped by card issuers more quickly, with a lower average loss per case (£381 in 2010 down to £226 in 2019 and £203 in 2020).

Cash use

In the first half of 2020, the COVID-19 pandemic led to reduced reliance on cash in order to limit the risk of contracting the virus by handling currency. To minimise these risks, the use of contactless payment cards has been promoted and increased limits on them before PIN has to be used. In the UK, contactless fraud on payment cards and devices remains low with £16m of losses during 2020, on spending of £9.46b over the same period (UK Finance, 2021). In less than a year since contactless limits increased across Europe to cope with the pandemic, Visa processed one billion additional PIN-free transactions.[11]

Economic stimulus fraud

Some types of fraud have a clear, causal relationship to the onset of the pandemic and the associated economic crisis. The clearest examples of this relate to dishonest attempts to obtain government economic stimulus funding, and payments made to support individuals who have lost jobs during the pandemic.

11 https://www.visa.co.uk/about-visa/newsroom/press-releases.3088603.html

Stimulus payment fraud in the United Kingdom

At the time of writing, the United Kingdom has not published data on the extent of COVID-19 stimulus fraud. In the United Kingdom, stimulus programs include the Coronavirus Job Retention Scheme and Bounce Back Loan Scheme for businesses. Workers covered by the Job Retention (Furlough) Scheme were not permitted to work for their employer while on the scheme, but some did. The government created a fraud reporting line to detect cases of fraud and error, and by 11 August 2020, 7,791 reports of alleged fraud had been made to the government (Rodger 2020), rising later (National Audit Office, 2020a, b; 2021a, b). There continued to be potential for employers to pressure furloughed employees to work for them covertly without pay or for only partial payment, since the government was paying most of their salaries.

In addition to the Job Retention Scheme, which had paid £64 billion by May 2021, the UK government provided so-called Bounce Back Loans that enable eligible business to apply for a 100 percent, state-backed loan of up to £50,000 per business, with no interest charged or repayments due during the first 12 months. By end May 2021, the UK government had backed loans of nearly £80 billion to businesses (https://www.gov.uk/government/news/final-covid-loans-data-reveals-80-billion-of-government-support-through-the-pandemic).

It has been alleged that loans have been provided with inadequate due diligence by banks and that some businesses have used funds for non-business purposes. Loans are also thought to have been provided to dormant or illegitimate businesses that are likely never to make repayments, and multiple payments made to the same applicant. Fraudsters have taken over business premises which were or are unoccupied. The fraudster targets these empty properties using a recently set up company for the purpose of making a grant claim and provides false lease agreements (containing the correct landlord details), utility bills and bank statements.

Corruption in procurement

Risks of corruption arising from the pandemic are likely to be significant, but they will take time to emerge and may often be 'explained away' as merely short-circuiting procedural rules. Pressures were placed on public officials to undertake procurement on a wide scale at speed to ensure that essential supplies such as Per-

sonal Protection Equipment, ventilators, vaccines and IT supplies for remote working were provided quickly. Although some procurement has managed to follow conventional risk-management policies appropriately, weaknesses in some processes used to speed up purchasing have been revealed, allowing for fraud and corruption and VIP-preferential opportunities to be exploited. Crowd-funded legal action has led to some of these arrangements being heavily criticised by the English courts in 2021 (https://goodlawproject.org/); others may keep the new European Public Prosecutor's Office busy in 22 MS: Hungary, Poland and Sweden have decided not to join the EPPO. Denmark and Ireland have opted out of all measures.

Best practice in preventing economic crimes

How, then, can governments, police, business and the community take action to minimise the risks of economic crime and fraud during pandemics? Some solutions are well known, already in use, but not fully implemented, while others remain to be developed.

Establishing and maintaining public sector fraud controls

Ongoing reviews need to be undertaken of national fraud control systems to ensure that they remain fit-for-purpose during times of economic shocks and pandemics. The lessons for fraud control that have been learnt during previous pandemics need to be understood and taken into account as fraud risk assessments are undertaken and fraud control plans revised.

In the UK, the government released its functional standard on countering fraud in October 2018, which sets out the expectations for the management of fraud, bribery and corruption risk in government organisations. 123 public bodies have adopted the standard (Cabinet Office, 2020), though the standard needs to be translated into action to have any effects. Specific principles for effective fraud control in response to pandemic threats are outlined, including using fraud risk assessments, having consistent data management systems in place, ensuring that funds paid incorrectly can be recovered, identifying applicants effectively, using cross-entity data-matching tools, and developing post-event assurance processes (Government Counter Fraud Function, 2020).

In addition, ongoing national pandemic planning exercises by government disaster management entities need to include risks of economic crimes and fraud – and provisions for their policing - as part of the response measures needed to deal with pandemics. Too often, fraud risk assessments only occur after a disaster, once many incidents of fraud have been detected and assessed—sometimes long after the event.

Monitoring fraud risks

It is also important to have adequate fraud monitoring and testing programs in place that are detailed enough to detect new instances of fraud during a pandemic, *as soon as they arise*. In the United Kingdom, police recorded crime statistics show between April 2019 and April 2020, fraud and computer misuse crimes fell by 16 percent. A general public telephone survey showed comparisons between the United Kingdom's lockdown period of April and May 2020 and the preceding two months showed an eight percent decline in fraud and a 57 percent increase in computer misuse incidents (Office of National Statistics, 2020); but later comparisons of the years to December 2020 showed very modest fraud differences year on year (Office of National Statistics, 2021). Data from police-run Action Fraud (2020) showed a 38% increase in "online shopping and auctions" fraud in the latest year (86,984 offences), plausibly from the increase in online shopping because of shop closures and fears of shopping during national lockdowns. The data also showed a 68% decrease in "ticket" fraud (2,532 offences), plausibly attributable to cancellation of live music events. "Hacking – social media and email" saw a 26% increase from 11,101 to 14,004 offences and "computer viruses and malware" saw a 30% increase from 5,536 to 7,192 offences between the years ending December 2019-2020.

One of the features of the coronavirus pandemic was the quick action taken by fraudsters to exploit opportunities created by the pandemic. Consumer scams using COVID-19 scenarios were developed as soon as the virus became apparent and frauds targeting government relief and stimulus programs also began as soon as these programs were implemented. Having effective real-time monitoring of fraud trends is essential to limit the extent to which opportunities for fraud are exploited. Reducing the *scale* of frauds and the amount of time available to spend or hide the proceeds is important, even if the *number* of frauds is not reduced.

Enhancing technology

Technological 'solutions' also need to be developed and implemented prior to pandemics taking hold. The NCSC (2021) noted that more than 11,000 UK-government-themed phishing campaigns were taken down – more than double the 2019 figure. The Suspicious Email Reporting Service was launched in April 2020, and received nearly 4 million reports by year-end, leading to the removal of over 26,000 scams not previously identified by the Takedown Service. The most phished UK government brand was Her Majesty's Revenue and Customs (HMRC). Equivalent data EU-wide are not yet collated or available, but many frauds are transnational and it would be surprising if the problems and their remedies were not universal.

Policing and prevention of frauds

Though there have been efforts during previous pandemics to discredit fake cures, the COVID-19 one is the first time that serious and systematic governmental and private sector efforts have been made to combat frauds, and the first occasion that large funds have been made available by governments to support businesses and people, though these have varied between Member States and beyond. These prevention efforts are connected to the risks to health and to savings, especially via the Web and social media apps, which provoked a more proactive response from governments and the private sector. (Though less is currently known about the reactions within the EU, beyond the efforts of Europol to communicate risks and engage in cross-border actions, than about the UK.)

Though the UK police have not received much extra funding for pandemic and government loan frauds, the UK tax agency HMRC has been given dedicated resources to pursue government loan frauds, and a range of UK bodies are actively engaged in fraud monitoring and prevention. Critical UK National Audit Office reports note the fraud implications of hasty government spending programs with inadequate due diligence on suppliers and borrowers, and apparent priority being given to those with government connections irrespective of their expertise (Public Accounts Committee, 2020, 2021). Reports to the HMRC fraud hotline rose to 121,300 in the year to March 2021 compared with 110,800 2019-20. The UK National Audit Office (2020b) found that 9 percent of people it surveyed admitted to working in lockdown at the request of their employer, and against the rules of the scheme. HMRC planned to tackle fraud through whistleblowing and retrospective compliance work. Setting aside the difficulties of distinguishing fraud from mistakes, the eventual net losses in all European and other jurisdictions will depend upon the capacity of the revenue agencies, insolvency practitioners and the criminal justice systems to recuperate the gross losses via tax demands, civil claims and proceeds of crime confiscation. However, we should not be too optimistic, as fraudsters spend a lot of money as they go along and recovery often takes years.

Should the policing of fraud during and after the pandemic get special priority? There is a sense in which when times are particularly upsetting (as with pyramid schemes in post-communist times) the police need to demonstrate to opportunists and to organised criminals that they are taking pandemic frauds very seriously, and offer both criminal investigation and public (including business) reassurance and resilience (Levi et al., 2017) to reduce feelings of anger and vulnerability. The data that have emerged so far relate primarily to volume frauds, but there are broader issues of social legitimacy in alleged favouritism and/or corruption by those with high connections that may have a longer term corrosive effect. This needs to be planned for. Building fraud control into future pandemic planning policies and activities will go a long way to ensuring that communities, businesses and governments are not taken by surprise when the next pandemic takes hold. But more and better economic crime policing is needed in Europe anyway because of the rise in fraud relative to other crimes that preceded the pandemic, and this will continue long after it stops. In addition to criminal investigation and prosecution, part of that policing is cooperation with businesses and individuals in the private sector and with other public bodies as part of a drive to manage frauds down.

Acknowledgements

This research is drawn from work funded by the British Academy (SRG20\201612), the UK Economic and Social Research Council Partnership for Conflict, Crime and Security Research (ES/S008853/1) and the Australian Institute of Criminology, from whose major report, Levi, M. and Smith, R.G. (2021), *"Fraud and its relationship to pandemics and economic crises: From Spanish 'Flu to COVID-19"*, *Research Report*, No. 19. Canberra: Australian Institute of Criminology, this paper has been adapted and given a more European focus.

References

- Action Fraud (AF), (2020), "UK Finance reveals ten Covid-19 scams the public should be on high alert for", London: Action Fraud.
  Available at: https://www.actionfraud.police.uk/news/uk-finance-reveals-ten-covid-19-scams-the-public-should-be-on-high-alert-for (Accessed 26 June 2021).
- Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021) Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.
- Cabinet Office, (2020) *Government functional standard GovS 013: Counter fraud: Counter fraud, bribery and corruption*. London: HM Government.
  Available at: https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud (Accessed 26 June 2021).
- Europol (2020) *Catching the virus: Cybercrime, disinformation and the COVID-19 pandemic*. The Hague: Europol
- Europol (2021) *SOCTA: A Corrupting Influence*. The Hague: Europol
- Felbab-Brown, V. (2020) "Order from chaos: What coronavirus means for online fraud, forced sex, drug smuggling, and wildlife trafficking", Brookings, 3 April.
  Available at: https://www.brookings.edu/blog/order-from-chaos/2020/04/03/what-coronavirus-means-for-online-fraud-forced-sex-drug-smuggling-and-wildlife-trafficking/ (Accessed 26 June 2021).
- Government Counter Fraud Function (2020) *Fraud control in emergency management: COVID-19 UK government guidance*. London: UK Government.
  Available at: https://www.gov.uk/government/publications/fraud-control-in-emergency-management-covid-19-uk-government-guide (Accessed 26 June 2021).
- Horgan, S., Collier, B., Jones, R. & Shepherd, L. (2020) 'Re-territorialising the policing of cybercrime in the postCOVID-19 era: towards a new vision of local democratic cyber policing', *Journal of Criminal Psychology*. 11 (3), pp.222-239. DOI: https://doi.org/10.1108/JCP-08-2020-0034.
- Keller, M.H. & Lorenz, T. (2020) "Coronavirus spurs a wave of suspect websites looking to cash in", *New York Times*, 24 March.
  Available at: https://www.nytimes.com/2020/03/24/business/coronavirus-ecommerce-sites.html (Accessed 26 June 2021).
- Levi, M., Doig, A., Gundur, R., Wall, D. & Williams, M. (2017) "Cyberfraud and the implications for effective risk-based responses: Themes from UK research", *Crime, Law and Social Change* Vol 67 No. 1, pp. 77–96
- Levi, M. (2008) *The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud*, 2nd edition, Andover: Ashgate.
- Levi, M (2017) 'Assessing the trends, scale and nature of economic cybercrimes', *Crime, Law and Social Change*, 67(1): 3-20.
- Levi, M. & Burrows, J. (2008) 'Measuring the impact of fraud: a conceptual and empirical journey', *British Journal of Criminology*, 48(3), pp. 293-318.
- Levi, M. & Smith, R.G. (2021) "Fraud and its relationship to pandemics and economic crises: From Spanish 'Flu to COVID-19'", in *Research Report*, No. 19. Canberra: Australian Institute of Criminology
- National Audit Office (NAO) (2020a) *Investigation into the Bounce Back Loan Scheme*. London: NAO
- National Audit Office (NAO) (2020b) *Implementing employment support schemes in response to the COVID-19 pandemic*. London: NAO
- National Audit Office (NAO) (2021a) *Good practice guidance: Fraud and Error*. London: NAO
- National Audit Office (NAO) (2021b) *Initial learning from the government's response to the COVID-19 pandemic Cross-government*. London: NAO
- National Cyber Security Centre (NCSC) (2020) *Annual review 2020*. London: NCSC.
  Available at: https://www.ncsc.gov.uk/news/annual-review-2020 (Accessed 26 June 2021).
- National Cyber Security Centre (NCSC) (2021) *Active Cyber Defence: the Fourth Year*. London: NCSC.
  Available at: https://www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf
- Office of National Statistics (ONS) (2020) *Coronavirus and crime in England and Wales: August 2020,* London: ONS.
  Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/coronavirusandcrimeinenglandandwales/previousReleases (Accessed 26 June 2021).
- Office of National Statistics (ONS) (2021) *Crime in England and Wales: year ending December 2020,* London: ONS.
  Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2020 (Accessed 26 June 2021).
- Public Accounts Committee (2020) *Covid-19: Bounce Back Loan Scheme*, HC 687, London: House of Commons.

- Public Accounts Committee (2021) *Fraud and Error: Ninth Report of Session 2021–22*, HC 253, London: House of Commons.
- Reitano, T. and Shaw, M (2021) *Criminal Contagion*, London: Hurst & Co.
- RiskIQ (2020) *A security checklist in the age of COVID-19 and the remote workforce.*
  Availabe at: https://www.riskiq.com/blog/external-threat-management/covid19-remote-workforce-checklist/ (Accessed 26 June 2021).
- Rodger, J. (2020) "HMRC issues furlough fraud update as investigators probe 8,000 claims", *Birmingham Mail*, 11 August.
  Available at: https://www.birminghammail.co.uk/news/midlands-news/hmrc-issues-furlough-fraud-update-18749262 (Accessed 26 June 2021).
- Ruiz, D. (2020) "Coronavirus scams, found and explained", *Malwarebytes Blog*, 19 March.
  Available at: https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/(Accessed 26 June 2021).
- UK Finance (2021) *Fraud: The facts 2021*. London: UK Finance.
  Available at: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf (Accessed 26 June 2021).
- Vu, A.V., Hughes, J., Pete, I., Collier, B., Chua, Y.T., Shumailov, I. & Hutchings, A. (2020) "Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras", In *Proceedings of the ACM Internet Measurement Conference* (pp. 551-566).
- Walker, S. (2020) *COVID-19 and crime: A response develops at the UN*. Geneva: Global Initiative Against Transnational Organized Crime.
  Available at: https://globalinitiative.net/analysis/covid-19-un-response/ (Accessed 26 June 2021).