Fraud and pandemics

Acknowledgements

This research is drawn from work funded by the Australian Institute of Criminology, the British Academy (SRG20\201612) and the UK Economic and Social Research Council Partnership for Conflict, Crime and Security Research (ES/S008853/1). The authors are grateful to the Australian Competition and Consumer Commission for providing current data on reported COVID-19 consumer scams in Australia.

Abstract

Purpose This article seeks to draw out the common characteristics of frauds associated with pandemics, and to identify any risks unique to them.

Design/methodology/approach It considers the range of frauds and their reporting lags, and examines what is known about current frauds against individuals, businesses and government, principally using public and private sector data from Australia and the United Kingdom.

Findings 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 regulatory guardians. It shows that many frauds would occur anyway, but some specific – mainly online - frauds occur during pandemics, and because of large scale government assistance programmes to businesses and individuals, far more opportunities were created from Covid-19 than in previous eras.

Originality The article uses fresh data on frauds from the private and public sectors, and assesses some measures of control in a holistic way.

Social and Policy implications. The article concludes with a discussion of the policy implications for prevention, resilience and for private and public policing and criminal justice. It stresses that plans for future pandemics must include provisions for better early monitoring and control of fraud and associated procurement corruption, and notes that these require greater political will and organisation. It recommends more serious analysis of the impact of prevention communications outreach to citizens, businesses and government.

Keywords

Covid-19, pandemics, fraud, corruption, prevention, cybercrime, tax fraud, policing.

Research Paper

Introduction

Frauds come in many forms, some of which have a prima facie connection to pandemics and others of which may not. The plausible direction of causality is important to consider. Do frauds exacerbate the effects of pandemics or even contribute to them in some parts of the world, e.g. via counterfeit medicines and false claims of effectiveness? Do health crises *always* generate opportunities for fraud, or are these risks connected to specific factors contingently developed in response to crises? Do pandemics change the fraudster population and how do they impact potential victim behaviour? What lessons have been learned, or not learned, from previous crises, and what are likely to be *actually* learned from the present one, though after every crisis and scandal, we usually say and perhaps believe we will learn lessons?

There is a 'dark figure' of undetected and detected but unreported and unrecorded frauds. This can vary from country to country and over time, but its precise dimensions are unknowable or contestable. The elapsed time from a fraud beginning to its formal detection and successful bringing to justice can take decades or, far more often, never happen. Large internal frauds and corruption usually take longer to surface and also to investigate and prosecute than volume frauds. This is a particular problem when analysing historical frauds since contemporary techniques of survey analysis and forensics are not readily used on them. The shift from mail and funds transfer via packet ships to Telegraph was the biggest time difference in fraud commission, though the web – whether email or fake advertising or social media - enables far less effort-per-fraud and has thus transformed fraud opportunities at a distance.

Changes in monitoring and policing or regulatory responses might be responsible for changes in official data, so we need to be wary of assuming that changes in reported or recorded 'fraud rates' are real reflections of underlying fraud behaviour. Likewise, the pandemic alters the shape of official responses. It might be expected that it would lead to less police investigation due to constraints on transport and face-to-face working: but some law enforcement agencies have used the opportunity to ramp up arrests, which have become more efficient since more domestic suspects are at home during lockdown than is normally the case. The hacking of encrypted criminal communications like Encrochat or the planting of pseudo-encrypted apps like ANOM might had more impact on economic crimes if distributed beyond drug trafficking networks: but this merely coincided with the pandemic.

Despite some level of regional and international harmonisation, we cannot assume that criminalisation of 'economic crimes' or fraud is universal and unchanging over time. For example, price gouging is not criminal everywhere, although it is a federal crime in the United States (see King and Spalding LLP, 2020). The UK Competition and Markets Authority (2020) has displayed a leisurely approach to the regulation of price increases, while in Australia regulators can deal with price gouging as a form of unconscionable conduct in some jurisdictions (e.g. Queensland Government, 2020). Elsewhere price gouging may be dealt with administratively if at all, and in a profit-driven economy there is legal and indeed ethical debate about the threshold for defining price setting as excessive 'gouging' (see e.g., House of Commons, 1919). There remain some contestable issues: when do homeopathic and prescription 'cures' for which there is no good scientific evidence become criminal deceptions?

Finally, the article examines whether anything has been learned, or reasonably could be learned, from the economic crime and crime control responses that followed previous pandemics.

This article focuses primarily on the United Kingdom and Australia as the objects of study concerning the Spanish flu pandemic of 1918-19 and COVID-19 of 2019-21. Other pandemics, such as the Asian flu in 1957-58, the Hong Kong flu A (H3N2) of 1968 and Swine flu A (H1N1) or 2009-10 hit the above jurisdictions much less hard. Though there have been efforts during each pandemic 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 that large funds have been made available by governments to support businesses and people. These efforts are connected to the perceived risks to health and financial behaviour, especially via the Web and social media apps, which provoked a more proactive response from both government and the private sector.

Fraud during the Spanish Flu pandemic

The major books and journal articles on Spanish flu mention fraud or corruption only as metaphors. In Seattle, one social elite funeral director was acquitted after a retrial of defrauding the US government by burying sailors in cheap caskets instead of the lined ones stipulated in his contract, and of writing to grieving families asking them to pay for coffins the government had already paid for (Berger, 2020). In general, historians of Spanish flu have focused not on scams but on the role of otherwise legitimate corporations in making false claims that their products could prevent and/or alleviate Spanish flu. It should be noted that this was a laissez-faire era that permitted other deceptive claims, including those promoting the health benefits of smoking tobacco (Health Administration Degree programs, 2020; Stanford University, 2020).

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. As the *Economic Outlook* of the OECD (2021) notes, the accumulation of household financial assets last year may have only a limited impact on private consumption, leaving more money available for investment. This, we add, includes investments that turn out to be frauds. When nominal interest rates are very low, offers of higher returns from markets (including cryptocurrencies) become even more attractive.

The shift towards the use of online platforms and teleworking during the 2019-21 pandemic has underlined the opportunities to offenders 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. The OECD (2021) notes that in the United States, as in other countries, better-educated, older and full-time workers in business services have been more easily able to telework than younger, less-educated and part-time workers.

Quantifying the problem

Quantification of the problem is hampered by a number of factors. First is the problem of determining the causal relationship between the pandemic and those frauds that *are* detected during or after it. As in previous pandemics, the disruption caused to business operations often simply results in existing frauds being uncovered—or, in the words of Warren Buffett (2018), 'You only learn who has been swimming naked when the tide goes out—and what we are witnessing at some of our largest financial institutions is an ugly sight.' Although the financial incentives for exposure are weak, as businesses go into receivership and liquidation, many pre-existing illegal activities are uncovered, though many remain unprosecuted (Association of Certified Fraud Examiners, 2020).

Evidence for this comes from the number of companies that have entered external administration. During the pandemic, many companies that normally would have failed were artificially supported by government payments, resulting in numbers entering external administration declining (ASIC, 2021, Insolvency Service, 2021). Once government support payments decline or end, we can expect that these numbers will increase considerably.

Although not necessarily indicative of fraud, some corporate failures may have occurred through phoenix activity, which continues to exist in Australia and Europe, despite various initiatives being used to minimise risks of this kind (eg Australian Taxation Office (ATO), 2020a). 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.

The second difficulty in quantifying fraud arising from pandemics is that fraud often takes many years to discover, and even longer for allegations to be investigated by police, dealt with in the courts (whose proceedings are delayed in times of pandemics), and appear in official statistics of recorded crime or convictions (if ever). For these reasons, other sources of data need to be relied on including consumer complaints, and both individual and corporate victimisation surveys. In Australia,

government agencies have embarked on a number of monitoring programs, not only to document the spread of the virus but also to document reports of pandemic-related consumer scams, false advertising and other forms of illegality (ACCC, 2021).

For example, the Australian Taxation Office indicated in July 2020 that 3,000 staff were reviewing applications for JobKeeper and other COVID-19 stimulus measures including auditing and data-matching to detect fraudulent payments (Khadem, 2020). Although few extra police fraud resources have been funded to date, the UK 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. The UK National Audit Office and the US General Accounting Office have already issued reports noting the fraud implications of hasty government spending programs with inadequate due diligence on suppliers and borrowers (see, for example, National Audit Office, 2020a, 2020b, 2021a, 2021b).

The National Audit Office warned that UK taxpayers could lose £15b to £26b from fraud, organised crime or default on the Bounce-Back Loans scheme alone, and Her Majesty's Revenue and Customs (HMRC) suggested that up to 10 percent of the money delivered by the scheme to mid-August, or £3.5b, may have been paid out in fraud or error (Public Accounts Committee, 2020). On average 10,000 calls per month were made to HMRC's hotline from April to December 2020, an increase of around 1,000 calls per month on the previous years' monthly average. 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. However, employees would not have known if their employer was part of the furlough scheme unless their employer had informed them, and HM Treasury refused to publish these data. HMRC intends to publish the names of employers claiming the new Job Support Scheme and to notify employees through their personal tax accounts when an employer has claimed job support. Setting aside the difficulty of distinguishing fraud from mistakes, the eventual net losses in both jurisdictions will depend upon the capacity of the revenue agencies, insolvency practitioners and the criminal justice system to recuperate the gross losses via tax demands, civil claims and proceeds of crime confiscation.

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; 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. Two principal vectors have involved dissemination of consumer scams and the commission of payment system fraud.

UK tabloid and broadsheet media stories anticipated a boom in frauds from the pandemic, focussed largely on public-facing scams but also on working from home. Phishing emails purporting to come from the US Centers for Disease Control and Prevention and the World Health Organization contained information about the coronavirus, but also links to malicious websites, or malware that permitted access to personal information. In addition to phishing, criminals quickly adapted conventional online scams to the coronavirus pandemic using various advance fee frauds, investment scams, charity and fundraising frauds, sale of non-existent or defective products and services, and illegal price gouging associated with PPE, safety and treatment products to deal with the virus (Zirkle, 2020). As time went on, ongoing working from home and social restrictions led to a boom in pet ownership: a UK survey published March 2021 stated that 2.1m (19%) collected a new pet in lockdown, and 1.8m (16%) planned to get one (https://www.pfma.org.uk/news/pfma-confirms-dramatic-rise-in-pet-acquisition-among-millennials-). This stimulated a wave of frauds

about the backgrounds of animals, and scams on those who had lost pets or had them stolen and advertised for their return. In Australia, puppy and other pet scams quintupled between 2019 and 2021 resulting in losses of over A$2.2m being sustained in 2020 alone (ACCC, 2021).

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. 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).

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 and 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. However, most fraud cases had nothing directly to do with Covid-19. In the year to April 2021, the City of London police stated that over £63m was lost nationally by victims of investment fraud who referred to a social media platform; 5,039 reports of investment fraud made reference to a social media platform, 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 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 (Action Fraud, 2020a).

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.

The national reporting system for phishing emails begun April 2020 was used heavily and in a sustained way. 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 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 coronavirus updates, local testing stations, potential cures, cheap medical products or working from home (IDCARE 2020). 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, 2020b). 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. Examples include the fabrication of a false version of Johns Hopkins University's COVID-19 interactive map using a domain

created by cybercriminals (Cuthbertson, 2020). In another case, a user-initiated thread on Russian-language cybercriminal forum XSS advertised a method of delivering malware via an email attachment disguised as a distribution map of the coronavirus outbreak containing real-time data from the World Health Organization. The offer was priced at US$200 for a 'private build', and if buyers also required a Java CodeSign certificate the price would be US$700 (Guirakhoo, 2020). 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.

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).

In Australia, between 1 March 2020 and 30 May 2021, more than 309m COVID-19 related consumer scams worth over $11m were reported to the ACCC's Scamwatch reporting portal (www.scamwatch.gov.au). Although representing only a small proportion of all scams reported to Scamwatch during this period, the reports that mentioned 'COVID', 'Coronavirus', or 'Corona' in contexts where it referred to the virus commenced almost immediately following the onset of the pandemic in early 2020. Unpublished data provided by the ACCC show the substantial increases in COVID-19 related scams reported during this period, in terms of both numbers and dollar losses **(Figure 1 here).**

Technology has also facilitated the sale of medical supplies and PPE during the coronavirus pandemic in 2020. A caveat is in order: data on fake availability tell us little about market size of fakes as a proportion of those purchased. Australian research has found vendors on the darknet selling PPE and drugs marketed as coronavirus vaccines or cures at high costs. In this study, 20 Tor darknet markets (not publicly visible—see Broadhurst et al., 2020) were surveyed on 3 April 2020 to ascertain the extent of COVID-19 related medical products and supplies. There were 645 listings, including 222 unique listings, of COVID-19 related products across 12 markets. 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.

Payment card fraud

While corporate insider and investment frauds and interpersonal scams of different kinds have been present for centuries, payment card technologies have made possible particular types of fraud, which have changed as both card use and technology has shifted since the 1980s.

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).

In the United Kingdom, changes in payment card use reflect shifts in criminal skills and also crime prevention and policing controls, including the ongoing decline in counterfeit card usage, as chip-

and-PIN makes card data less useful for criminals, and the huge increase in remote purchase frauds through e-commerce is reflected in card-not-present fraud **(Table 1 here**).

In the UK, card fraud losses as a proportion of the amount spent on UK-issued cards increased during 2020 (UK Finance, 2021). The fraud to turnover ratio is higher than it was a decade ago, though with fluctuations up and down in between. 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).

In Australia, national payment card fraud statistics are published by the Australian Payments Network (AusPayNet, 2020a). As in the UK, fraud on payment card transactions has continued to decline, although fraud involving lost and stolen cards in which PINs were not used (contactless) have increased substantially (**Figure 2 here**). This trend is likely to continue as the coronavirus pandemic progresses.

Comparing the UK with Australia in 2019, card fraud as a percentage of all card spending was 0.075 percent in the UK and 0.057 percent in Australia. Card fraud was 75 percent of all payment fraud in the UK and 92 percent in Australia, and card-not-present fraud was 76 percent of all card fraud in the UK and 87 percent in Australia (AusPayNet 2020). In both countries, industry initiatives have created a general decline in card fraud, making the actual effect of the pandemic difficult to quantify in the short-term.

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. Contactless fraud on payment cards and devices represents 2.9 percent of overall card fraud losses, while 55 percent of all card transactions were contactless in 2019 (UK Finance, 2021).

Economic stimulus fraud

Some types of fraud have a clear, causal relationship to the onset of the pandemic and the associated economic crisis. In Australia and the UK, 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 or property during the pandemic or, in Australia's case, natural disasters such as the bushfires in 2019–20 (Fowler, 2020).

Stimulus payment fraud in Australia

In Australia, the COVID-19 pandemic led to a substantial increase in government-funded support payments being made, e.g., the *Coronavirus Economic Response Package Omnibus Act 2020* (Cth). On 1 May 2020, the ATO (2020b) issued compliance guidelines in relation to schemes involving JobKeeper payments. Designed to assist taxpayers, the guidelines gave details of eight scenarios in which the JobKeeper payment scheme could be compromised, some entailing complex dishonest activities. In 2020, 24 allegations of fraud involving pandemic stimulus payments were referred to the Australian Federal Police. In two cases, those accused were charged with fraudulently claiming $27,000 using 25 assumed identities. In other cases, businesses have registered for JobKeeper payments but illegally withheld a proportion of the funds from their employees (Palmer-Derrien, 2020). Following a review of the support payment programs, additional measures are being taken to ensure that payments are made to those most in need of support.

Again, such opportunistic frauds started soon after the pandemic began, with some complex and elaborate strategies used to obtain funds illegally. Two of the largest government support programs, JobKeeper and JobSeeker, have created opportunities for ineligible individuals and businesses to

defraud these schemes, with the ATO rejecting 6,500 applications for JobKeeper payments alone due to fraud or error (Treasury 2020a, 2020b).

Another government initiative enabled individuals to withdraw up to $20,000 over two months from personal superannuation savings, which are normally preserved until retirement age. Following the introduction of this economic stimulus measure, designed to support those who had lost jobs, some $30b was withdrawn, representing one percent of all Australian superannuation holdings. The ATO and Australian Federal Police are aware of at least 150 cases of COVID-19 related identity fraud, in which individuals allegedly attempted to obtain early access to superannuation funds fraudulently (Roddan, 2020).

A third source of support payments enabled small businesses and not-for-profit organisations to claim between $20,000 and $100,000 as a cash flow boost to help them maintain operations during the pandemic. Again, some payments were made to those outside the eligibility rules.

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 (Tew 2020; Welford 2020), 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, 2020b). There continues 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 August 2020, more than 1.5m businesses had borrowed up to £50,000 each, worth a total of £35b.. By 21 March 2021, the Coronavirus Business Interruption Loan Scheme approved £23.28 bn; the Coronavirus Large Business Interruption Loan Scheme approved £5.3 b; and the Bounce Back Loan Scheme, £56.53b in expenditure (HM Treasury, 2021).

It has been alleged that loans have been provided with inadequate due diligence by banks and that some businesses have sought to use 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.

The scale of the fraud remains to be quantified and will only become apparent once the time for repayment begins (Cahill, 2020; Sproson, 2020). HM Treasury rejected a UK Fraud Advisory Panel proposal requesting that the government increase transparency around the Bounce Back Loans and Coronavirus Business Interruption Loan Schemes by publishing the names of all companies that have received the loans: it is hard to see how their publication would have impeded economic recovery. Although not yet quantified, the scale of fraud and error involved in these programs, in both Australia and the United Kingdom, is costly. Most of the media and political pressures in the first year of the pandemic have been on the non-provision or delayed provision of aid to needy businesses and individuals rather than on fraud risk reduction, though individual cases of abuse and alleged procurement corruption or ‘chumocracy’ have received and will continue to receive significant attention when published, as will any audit reports.

Corruption in procurement

Risks of corruption arising from the pandemic are likely to be high, but will take time to emerge. Pressures were placed on public officials to undertake procurement on a wide scale at speed to

ensure that essential supplies such as PPE, ventilators, vaccines and IT supplies for remote working are 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 taken by the Good Law Project has led to some of these arrangements being heavily criticised by the courts in 2021 (https://goodlawproject.org/). Governments in both the UK and Australia are monitoring these risks as the pandemic progresses and it is expected that criminal and disciplinary action will be taken against some public officials as cases come to light. Again, lessons from previous pandemics – including better preparation for this one - could have been relied on to prevent some of the illegality and poor practice that has occurred.

Understanding pandemic-related fraud

Opportunity

Levi and Smith (2011) explored some of the explanations underlying economic crime in connection with the global financial crisis in 2008–09, applying Clarke's (2012) opportunity theory approach. Although this theory cannot account for all aspects of the current pandemic, government stimulus packages have created numerous opportunities for individuals to commit economic crimes. As was the case in the global financial crisis, some economic support measures were introduced quickly with inadequate fraud controls, creating sometimes simple ways in which to obtain payments from governments dishonestly or in breach of eligibility criteria. Some who committed such frauds may have been motivated by need arising from loss of employment, or a desire to keep businesses trading until economies improve. Others, including existing and freshly recruited members of organised crime groups, saw the lack of fraud controls as a way to obtain wealth using often sophisticated strategies designed to avoid detection and prosecution.

Rationalisations and coping mechanisms

This article has not specifically analysed, first-hand, the motivations of Covid-19 fraud offenders, although it is clear from the above that coronavirus fraudsters are motivated by a mixture of economic need, stimulated by a decline in business activity and loss of jobs, and personal greed driven by opportunities to gain access to government support payments during a time of a perceived reduction in fraud controls as well as extra vulnerabilities generated by Working From Home and social isolation for individuals of varying ages. Nonetheless, some broader context appears worthwhile.

One of the principal components of the 'fraud triangle' and its variants as a framework for understanding fraud offending in organisations is the capacity of individuals to rationalise their conduct based on personal attitudes and situational pressures (Andon and Free, 2020; Schuchter and Levi, 2015). The 2020-21 pandemic, being global in its reach and causing widespread economic as well as health consequences, has created many rationalisations for fraud, including almost all of Sykes and Matza's (1957) techniques of neutralisation.

One of the most frequently relied on rationalisations for organisational fraud is the need to support a failing business to save employees' jobs and to maintain cash flow in the economy. During the pandemic, governments promoted this by providing payments to support businesses facing closure due to lack of consumer demand, such as the Australian JobKeeper payments. Business proprietors could therefore argue that their desire to support the economy and to help themselves and their staff survive was the main reason for acting dishonestly, and that even if funding was obtained inappropriately, it nonetheless helped to stimulate the overall economy. Evidence supporting this argument comes from Ernst and Young (2016) in its *14th global fraud survey*, which found that 36 percent of chief financial officers surveyed would rationalise unethical conduct in order to improve the financial performance of the organisation.

Capable guardianship

In addition to considering opportunity- and rationalisation-based elements of situational crime prevention, the absence of capable guardians is also relevant to the current pandemic. Guardians can act as an inhibiting factor in the decision to act illegally and/or to continue to do so, and their effective absence can provide an additional stimulus for acting dishonestly. During the pandemic, law enforcement priorities have shifted away from conventional policing to community support roles. For example, police have been directed to guard virus hotspots and issue fines to people breaching social distancing orders, leaving less time for conventional policing—particularly of economic crime. In addition, the complexities of new laws introduced to control the pandemic and to stimulate the economy make policing of economic crime in these times demanding.

Even during more stable economic times, resources for policing economic crime are stretched, but during pandemics the chances of detecting and seriously investigating fraud are limited. In Australia, although the ATO has made use of data matching and artificial intelligence systems to monitor stimulus payments (Hendry, 2020a, 2020b), law enforcement action has been limited, with few prosecutions arising. Over time, as the scale of fraud and error increases, it is likely that more resources will be devoted to official action—even if the courts are unable to deal with the backlog of cases awaiting hearing, and the need to use virtual courtrooms.

In the United Kingdom, there have been regular and ongoing criticisms of counter-fraud strategies and policing efforts at national and local levels (Doig and Levi, 2020; HM Inspectorate of Constabulary and Fire and Rescue Services, 2019; Levi and Doig, 2020). Although COVID-19 has stimulated strong efforts at intelligence-sharing and fraud reduction, and freed some police resources for increased arrests for high vulnerability offences such as courier fraud, overstretched resources at police and HMRC mean that only a modest number of strategically selected and opportunistic arrests can be made, now and plausibly in the future, when the extent of fraudulent and other losses on 'loans' becomes clearer. As in Australia, UK courts have large backlogs, partly due to the impact of social distancing measures on court attendance during the pandemic as well as austerity reductions in capacity, and there are processing difficulties that inevitably increase the delay between offence commission and possible justice outcomes. As Levi et al. (2017) and Dupont (2019) argue in the case of cyber-enabled frauds, where the capacity for pursuing crime is limited, a systematic focus on resilience and prevention is vital.

Larger organisations handling a lot of sensitive data have implemented systematic security processes for remote working (especially as this is now seen as a long-term practice), but relatively low-cost attempts at business email compromise, data breaches, and ransomware have become commonplace. In the United Kingdom, the National Cyber Security Centre has enhanced a suite of prevention advice and reporting mechanisms for individuals and business. UK Finance, individual banks, and cross-sectoral bodies such as Cifas have enhanced their intelligence and confirmation of payee processes to make diversion frauds harder. Newspapers and consumer programs on radio and television, however, testify to the incompleteness and imperfection of these processes, as well as to inconsistencies in victim compensation (Barrett, 2021; Maunder, 2021). In public-facing, inter-business, and intra-public sector areas, liaison and information sharing efforts have expanded as part of the reaction to expected increases in fraud during the COVID-19 pandemic.

Another form of guardianship that has taken on importance in preventing and uncovering fraud during pandemics is that of natural surveillance. Individuals in workplaces or in the community generally are often able to detect behavioural anomalies that could indicate fraud and report them to the authorities. In a time of crisis, the need for communities to act collaboratively means reporting suspected illegality may be more likely to occur than in more settled times. In the United States, for example, whistleblowers who report suspected fraud against government-funded programs can receive incentive payments. Recently, they have been alerted to the possibility of taking action and have reported COVID-19 related fraud under the US *False Claims Act* (31 USC ss 3729–33). This has occurred in cases of conspicuous spending of government-funded Paycheck Protection Program payments on lifestyle goods and services, gambling and cryptocurrencies (Johnson, 2020). In the United Kingdom, many thousands of workers have reported suspected fraud

by their employers relating to the Coronavirus Job Retention Scheme, as noted above (Welford, 2020). In one case, a man was arrested in relation to a suspected Job Retention Scheme fraud involving £495,000 (Tew, 2020).

Best practice in preventing fraud in future pandemics

How, then, can governments, 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. The following are some examples of best practice initiatives that could be adopted to minimise risk of fraud in future pandemics.

Establishing national 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 Australia, the Commonwealth Fraud Prevention Centre (Attorney-General's Department, 2020) has monitored fraud risks for the Commonwealth. In addition, the Australian Institute of Criminology's annual Fraud against the Commonwealth Census required respondent entities in September 2020 to indicate how their fraud controls have changed in response to the risks uncovered during the COVID-19 pandemic. The results of this census should be used alongside reviews of actual fraud levels to develop appropriate fraud control measures for the years ahead. The Commonwealth Fraud Prevention Centre (Attorney-General's Department, 2020) also provides guidance on counter-fraud activities recommended for entities during the pandemic.

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. As of February 2020, 123 public bodies had adopted the standard (Cabinet Office, 2020), though the standard is not self-implementing. Dealing with the specific risk of fraud arising from the COVID-19 pandemic, specific guidance has been provided on how to respond to threats, particularly of misrepresentation when applying for government grants and third parties impersonating businesses to obtain grant funding. 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 crime and fraud 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 a considerable time after the event. A comprehensive plan to prepare for a disaster should include predicting the likely fraud and economic crime risks that will arise, based on previous experience, and developing control measures to ensure that these risks are addressed prior to the crisis occurring.

Monitoring fraud risks

It is also important to have adequate fraud monitoring and testing programs in place that are of sufficient granularity 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. Experimental statistics were also published of the Telephone-operated Crime Survey for England and Wales. 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 Action Fraud (2020b) 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—though there is no evidence yet that these led to a net increase in such consumer scams—and frauds targeting government relief and stimulus programs also began as soon as these programs were implemented. This was partially because of the necessity for some individuals and businesses to support their failing financial positions by securing alternative sources of funding, but also because of the complexity of eligibility rules, which changed rapidly and were poorly administered in some jurisdictions. 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 squirrel away 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. Although primarily introduced as a health measure, in both Australia and the United Kingdom, contact-tracing applications were developed, but were not suitable for all smartphone systems and, more importantly, take-up by the community was less than needed owing to concerns over data confidentiality and function creep. Use of the app data for fraud control could, arguably, be one of the types of function creep that citizens feared.

Extensive data-matching using artificial intelligence algorithms was undertaken by the Australian Government in order to detect fraud and error in connection with pandemic relief and economic stimulus programs. The ATO indicated in July 2020 that 3,000 staff were doing ongoing reviews of JobKeeper and other stimulus payment applications to ensure that applicants were adhering to eligibility rules. By July 2020, 6,500 applications for JobKeeper support payments had been rejected for suspected fraud or error (Khadem, 2020).

Responding to rationalisations

Many frauds are intentional acts committed with awareness that what is being done is illegal. However, governments and business need to address the various neutralisation techniques and coping strategies individuals use to justify their dishonest behaviour. One of Clarke's (1997) opportunity-reducing techniques of situational crime prevention is to remove excuses for acting illegally. This can be achieved in four ways that have direct relevance to the prevention of fraud during pandemics. Firstly, people who may be likely to act dishonestly need to know precisely what lawful conduct entails. During pandemics, when stimulus payments are often implemented quickly, individuals are often unclear about their obligations, such as eligibility for claiming funds from governments. Conflicting rules across jurisdictions also should be avoided, particularly in a country with a federal system such as Australia.

Secondly, governments could emphasise the social utility of adhering to rules and could make clear the moral obligation or social contract that obliges members of the community not to act fraudulently for personal gain. In terms of tertiary crime prevention using the criminal justice system, public shaming undertaken in a reintegrative way (Braithwaite, 1989) could have potential benefits for minimising recidivism (Levi, 2002). Thirdly, technological solutions could also be used to control disinhibiting factors. In the case of fraud control, making dishonest payments impossible or detecting them quickly through the use of data analytic methods is one viable option.

Finally, helping those in the community to achieve compliance would prevent rationalisations based on arguments such as 'I didn't know that what I was doing was illegal' or 'The eligibility rules were too complicated to understand.'

Learning from the past

Finally, we need to learn from previous pandemics. If knowledge of the past had been collated and used effectively, some of the present harms could have been avoided.

In 2020, as during the Spanish flu pandemic, each of the Australian states and territories responded differently to the infection risks they faced from COVID-19, with some closing borders sooner rather than later, and others having inadequate measures in place to prevent the spread of infections in specific communities and locations. The fraud risk arising from the pandemic generally affected Commonwealth interests, although the cross-border movement of people created difficulties for policing and enforcement. Many issues that arose in the current pandemic were similar to those experienced in 1919 (see Bongiorno, 2020; McQueen, 1976), particularly the limitations of Australia's federal system of government and the difficulties of monitoring movements across borders—despite attempts to use digital tracking solutions that were unavailable in 1919. Devolution in the UK is much more recent, and it is less clear what effects it had on fraud, not least since the loan schemes were primarily central government in their administration.

Ideally, the nature and extent of fraud that occurred in previous pandemics need to be documented and understood so that similar risks can be avoided in the future. Although each has its own unique characteristics, there are many common themes and risks that fraudsters can exploit. Ensuring that these are identified and counter measures implemented in advance of new crises could result in considerable savings for governments and the community—arguably, easily off-setting the predicted costs of fraud that are likely to be experienced. 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.

Similarly, ensuring that fraud control plans and fraud risk assessments are regularly revisited will help to guard against many of the conventional fraud risks that are likely to occur. In addition, efforts need to be made to evaluate historical fraud control measures that have previously been tried to determine how successful they were in limiting fraud risks and reducing overall losses. 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. As Louis Pasteur noted in a lecture in 1854, 'In the fields of observation, chance favours only the prepared mind' (Vallery-Radot, 1919, p. 76).

References

URLs current as at July 2021

Action Fraud (AF), (2020a), "New figures reveal victims lost over 63m to investment fraud scams on social media", London: Action Fraud. Available at: https://www.actionfraud.police.uk/news/new-figures-reveal-victims-lost-over-63m-to-investment-fraud-scams-on-social-media (Accessed 26 June 2021).

Action Fraud (AF), (2020b), "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).

Andon, P. and Free, C. (2020), "Strain, coping and sustained fraud offending", *Trends and issues in crime and criminal justice* no. 596. Canberra: Australian Institute of Criminology. Available at: https://www.aic.gov.au/publications/tandi/tandi596 (Accessed 26 June 2021).

Association of Certified Fraud Examiners (ACFE), (2020), *Report to the nations: 2020 global study on occupational fraud and abuse*. Texas: ACFE. Available at: https://www.acfe.com/report-to-the-nations/2020/ (Accessed 26 June 2021).

Attorney-General's Department, (2020), *Counter fraud during the COVID-19 pandemic.* Canberra: Attorney-General's Department. Available at: https://www.ag.gov.au/integrity/counter-fraud/counter-fraud-during-covid-19-pandemic (Accessed 26 June 2021).

Australian Competition and Consumer Commission (ACCC) 2021. *Targeting Scams: Report of the ACCC o=n scams activity 2020*. Canberra: ACCC. Available at: http://www.scamwatch.gov.au/scam-statistics/targeting-scams (Accessed 26 June 2021).

Australian Cyber Security Centre (ACSC), (2020), "COVID-19 cyber security advice". Canberra: ACSC. Available at: https://www.cyber.gov.au/acsc/services/covid-19-cyber-security-advice (Accessed 26 June 2021).

Australian Payments Network (AusPayNet) 2021. *Australian payment card fraud 2020*. Sydney: AusPayNet. Available at: https://www.auspaynet.com.au/resources/fraud-statistics/July-2019-June-2020 (Accessed 26 June 2021).

Australian Payments Network (AusPayNet) 2020. *Australian payment fraud 2020*. Sydney: AusPayNet. Available at: https://www.auspaynet.com.au/resources/fraud-statistics/2019-Calendar-year (Accessed 26 June 2021).

Australian Securities and Investments Commission (ASIC), (2021), *Insolvency statistics – Series 1B: Notification of companies entering external administration.* Chart 1B.3. Available at: https://asic.gov.au/media/gtflak23/asic-insolvency-statistics-series-1b-weekly-update-published-8-june-2021.xlsx (Accessed 26 June 2021).

Australian Taxation Office (ATO), (2020a), *Phoenix taskforce*. Canberra: ATO. Available at: https://www.ato.gov.au/general/the-fight-against-tax-crime/our-focus/illegal-phoenix-activity/phoenix-taskforce/ (Accessed 26 June 2021).

Australian Taxation Office (ATO), (2020b), *Practical Compliance Guideline: Schemes in relation to the JobKeeper payment*. PCG 2020/4. Canberra: ATO. Available at: https://www.ato.gov.au/law/view/document?docid=COG/PCG20204/NAT/ATO/00001 (Accessed 26 June 2021).

Barrett, C. (2021), "Will we ever win the war on bank fraud?" *Financial Times*, 18 June. Available at: https://www.ft.com/content/31094703-7913-49e9-8b28-2a878bad9d29 (Accessed 26 June 2021).

Berger. K. (2020), "Shady landlords and bootleggers ruled Seattle's last pandemic", *Crosscut*, 7 April. Available at: https://crosscut.com/2020/04/shady-landlords-and-bootleggers-ruled-seattles-last-pandemic (Accessed 26 June 2021).

Bongiorno, F. (2020), "How Australia's response to the Spanish flu of 1919 sounds warnings on dealing with coronavirus", *The Mandarin*, 24 March. Available at: https://www.themandarin.com.au/128408-how-australias-response-to-the-spanish-flu-of-1919-sounds-warnings-on-dealing-with-coronavirus/ (Accessed 26 June 2021).

Braithwaite, J. (1989), *Crime, shame and reintegration*. Cambridge: Cambridge University Press

Broadhurst, R, Ball, M. and Jiang, C.J. (2020), *Availability of COVID-19 related products on Tor darknet markets*. Statistical Bulletin no. 24. Canberra: Australian Institute of Criminology. Available at: https://www.aic.gov.au/publications/sb/sb24 (Accessed 26 June 2021).

Buffett, W. (2018), "Who has been swimming naked?" Letter to Berkshire-Hathaway shareholders on 29 April 2007. *Buffettpedia*, 29 April. Available at: http://buffettpedia.com/2018/04/who-has-been-swimming-naked/ (Accessed 26 June 2021).

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).

Cahill, H. (2020), "Fraudsters raid Chancellor Rishi Sunak's loan fund—Probe finds criminal gangs exploit loopholes in £35bn business bounce back scheme", *Financial Mail on Sunday*, 23 August. Available at: https://www.dailymail.co.uk/money/markets/article-8653807/Fraudsters-raid-Chancellor-Rishi-Sunaks-loan-fund.html (Accessed 26 June 2021).

Clarke, R.V. (2012), "Opportunity makes the thief. Really? And so what?" *Crime Science* Vol 1, pp. 3–9. https://doi.org/10.1186/2193-7680-1-3

Clarke, R.V. (ed) (1997), *Situational crime prevention: Successful case studies*, 2nd ed. Albany, NY: Harrow and Heston

Competition and Markets Authority (CMA), (2020), *Joint statement against price gouging*. Available at: https://www.gov.uk/government/publications/cma-and-trade-bodies-joint-statement-against-price-gouging/joint-statement-against-price-gouging (Accessed 26 June 2021).

Cuthbertson. A. (2020), Coronavirus 'fearware' sees hackers exploit COVID-19 panic to target victims. *The Independent*, 13 March. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-hackers-covid-19-china-fearware-malware-a9400141.html (Accessed 26 June 2021).

Doig, A. and Levi, M. (2020), "Editorial: The dynamics of the fight against fraud and bribery: Reflections on core issues in this PMM theme". *Public Money and Management* vol 40 No 5, pp. 343–348.

Dupont, B. (2019), "The cyber-resilience of financial institutions: Significance and applicability", *Journal of Cybersecurity* Vol 5 No.1, pp. 1–17. DOI: 10.1093/cybsec/tyz013

Ernst and Young (2016), *14th global fraud survey*. London: Ernst and Young.

Europol (2020), *Catching the virus: Cybercrime, disinformation and the COVID-19 pandemic.* 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).

Fowler, M. (2020), "State's $100m plan for bushfire recovery". *Sunday Age*, 23 August: 2 (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).

Guirakhoo, A. (2020), How cybercriminals are taking advantage of COVID-19: Scams, fraud, and misinformation. *Digital Shadows,* 12 March. Available at: https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-COVID-19-scams-fraud-misinformation/ (Accessed 26 June 2021).

Health Administration Degree Programs (2020), "10 evil vintage cigarette ads promising better health", Available at: https://www.healthcare-administration-degree.net/10-evil-vintage-cigarette-ads-promising-better-health/ (Accessed 26 June 2021).

Hendry, J. (2020a), "AFP says third-party system intrusion behind early-access super fraud", *IT News*, 7 May. https://www.itnews.com.au/news/afp-says-third-party-system-intrusion-behind-early-access-super-fraud-547883 (Accessed 26 June 2021).

Hendry. J. (2020b), "ATO to match data for early access super scheme, JobKeeper crackdown", *IT News*, 23 June. Available at: https://www.itnews.com.au/news/ato-to-match-data-for-early-access-super-scheme-jobkeeper-crackdown-549600?eid=3andedate=20200629andutm_source=20200629_PMandutm_medium=newsletterandutm_campaign=daily_newsletter (Accessed 26 June 2021).

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) (2019), *Fraud: Time to choose: An inspection of the police response to fraud*. London: HMICFRS. Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/an-inspection-of-the-police-response-to-fraud/ (Accessed 26 June 2021).

House of Commons (1919), *Parliamentary Debates, Second Reading debate on the Profiteering Bill 1919*, 11 August 1919, vol 119, cc923–1027. Available at: https://api.parliament.uk/historic-hansard/commons/1919/aug/11/profiteering-bill-1 (Accessed 26 June 2021).

IDCARE (2020), *Homepage*. https://www.idcare.org (Accessed 26 June 2021).

Insolvency Service (2021), *Commentary - Monthly Insolvency Statistics May 2021.* Available at: https://www.gov.uk/government/statistics/monthly-insolvency-statistics-may-2021/commentary-monthly-insolvency-statistics-may-2021 (Accessed 26 June 2021).

Johnson, J. (2020), Vegas trips and Lamborghinis: How fraudsters defrauding government stimulus programs are being caught. *The Fraud Examiner*, 18 August. Available at: https://www.acfe.com/fraud-examiner.aspx?id=4295011053 (Accessed 26 June 2021).

Keller, M.H. and 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).

Khadem, N. (2020), "More than 6,500 applications for JobKeeper rejected due to ineligibility or fraud, ATO says". Available at: *ABC News*, 3 July. https://www.abc.net.au/news/2020-07-03/more-than-6500-applications-for-jobkeeper-rejected-due-to-fraud/12415670 (Accessed 26 June 2021).

King and Spalding LLP (2020), *COVID-19 survey of federal and state price gouging laws*. Available at: https://www.kslaw.com/pages/covid-19-survey-of-federal-and-state-price-gouging-laws (Accessed 26 June 2021).

Levi, M. (2002), "Suite justice or sweet charity? Some explorations of shaming and incapacitating business fraudsters", *Punishment and Society* Vol 4 No. 2, pp.147–63

Levi, M. and Doig, A. (2020), "Exploring the 'shadows' in the implementation processes for national anti-fraud strategies at the local level: Aims, ownership and impact", *European Journal on Criminal Policy and Research* Vol 26, pp. 313–333

Levi, M., Doig, A., Gundur, R., Wall, D. and 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. and 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

Levi, M. and Smith, R.G. (2011), "Fraud vulnerabilities and the global financial crisis", *Trends and issues in crime and criminal justice* no. 422. Canberra: Australian Institute of Criminology

Maunder, S. (2021), "Which? calls on regulator to make banks come clean about fraud refunds". Available at: https://www.which.co.uk/news/2021/06/which-calls-on-banks-to-come-clean-about-fraud-refunds/ (Accessed 26 June 2021).

McQueen, H. (1976), "The 'Spanish' influenza pandemic in Australia, 1912–19", In J Roe (ed), *Social policy in Australia: Some perspectives 1901–1975.* Sydney: Cassell Australia. Available at: https://labourhistorycanberra.org/2018/06/the-spanish-influenza-pandemic-in-australia-1912-19/ (Accessed 26 June 2021).

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 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 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).

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).

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).

OECD (2021), *OECD Economic Outlook,* Volume 2021 Issue 1: Preliminary version, No. 109, OECD Publishing, Paris, https://doi.org/10.1787/edfbca02-en.

Palmer-Derrien, S. (2020), "'Dob them in': Morrison lays down the law for employers thinking of pocketing the JobKeeper subsidy", Available at: https://www.smartcompany.com.au/coronavirus/warning-employers-jobkeeper-fraud/ (Accessed 26 June 2021).

Public Accounts Committee (2020), *Tackling the tax gap*. HC 650. London: House of Commons

Queensland Government (2020), *Disaster assistance: Profiteering and price gouging.* Brisbane: Queensland Government. Available at: https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/fair-trading-services-programs-and-resources/fair-trading-latest-news/disaster-assistance/profiteering-price-gouging (Accessed 26 June 2021).

RiskIQ (2020), *A security checklist in the age of COVID-19 and the remote workforce.* https://www.riskiq.com/blog/external-threat-management/covid19-remote-workforce-checklist/ (Accessed 26 June 2021).

Roddan, M. (2020), "AFP investigates early-access super fraud", *Australian Financial Review*, 6 May. Available at: https://www.afr.com/politics/afp-investigates-early-access-super-fraud-20200506-p54qjg (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).

Schuchter, A. and Levi, M. (2015), "Beyond the fraud triangle: Swiss and Austrian elite fraudsters", *Accounting Forum* vol 39, pp. 176–187

Sproson, K. (2020), "'Bounce back loans' – help for small businesses and income support for those missing out elsewhere, eg, limited company directors and self-employed". Available at: https://www.moneysavingexpert.com/news/2020/05/small-business-boost-as-bounce-back-loans-launched/ (Accessed 26 June 2021).

Stanford University (2020), "Blowing smoke: Vintage ads of doctors endorsing tobacco". Available at: https://www.cbsnews.com/pictures/blowing-smoke-vintage-ads-of-doctors-endorsing-tobacco/ (Accessed 26 June 2021).

Sykes, G.M. and Matza, D. (1957), "Techniques of neutralization: A theory of delinquency", *American Sociological Review* Vol 22, pp. 664–70. https://dx.doi.org/10.2307/2089195

Tew. I. (2020), "HMRC cracks down on furlough fraud with first arrest", *FT Adviser*, 31 July. Available at: https://www.ftadviser.com/your-industry/2020/07/13/hmrc-cracks-down-on-furlough-fraud-with-first-arrest/ (Accessed 26 June 2021).

Treasury (2020a), *Economic response to the coronavirus*. Canberra: The Treasury. Available at: https://treasury.gov.au/sites/default/files/2020-03/Overview-Economic_Response_to_the_Coronavirus_2.pdf (Accessed 26 June 2021).

Treasury (2020b) *The JobKeeper payment: Three month review*. Canberra: The Treasury. Available at: https://treasury.gov.au/publication/jobkeeper-review (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).

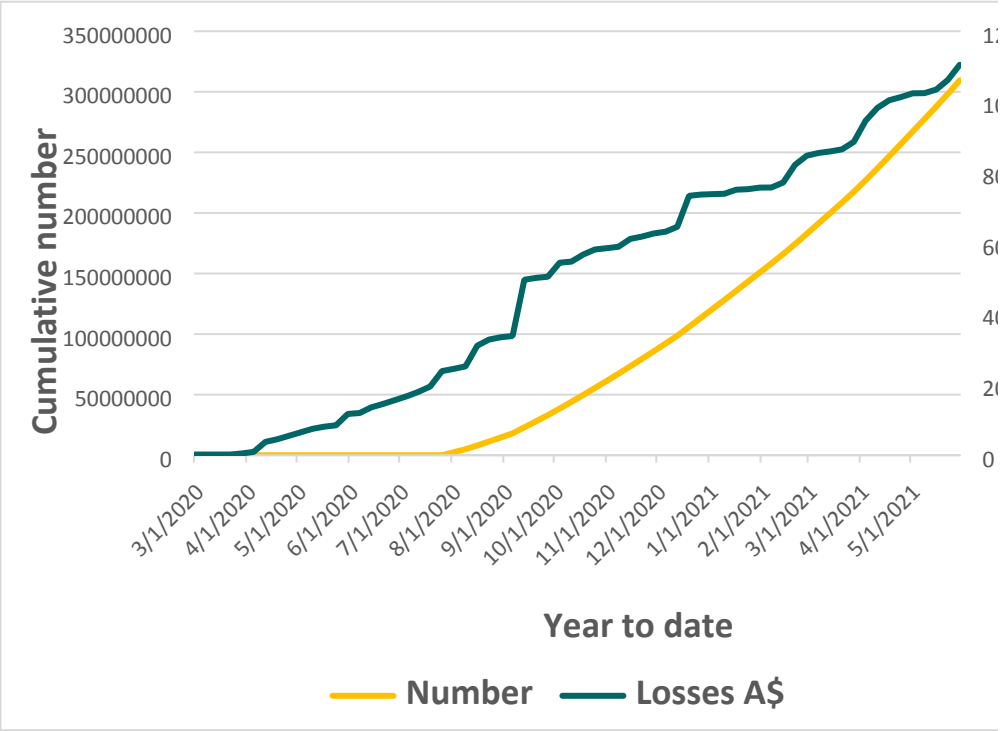
Vallery-Radot, R. (1919), *The life of Pasteur*, translated by RL Devonshire. London: Constable

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).

Welford, J. (2020), "HMRC: The thousands of reports of alleged furlough fraud made since the scheme started", *Teesside Live*, 1 August. Available at: https://www.gazettelive.co.uk/news/teesside-news/hmrc-thousands-reports-alleged-furlough-18675353 (Accessed 26 June 2021).

Zirkle, J. (2020), "Coronavirus fraudsters add to the anxiety and misery". Available at: https://www.acfe.com/article.aspx?id=4295010402 (Accessed 26 June 2021).

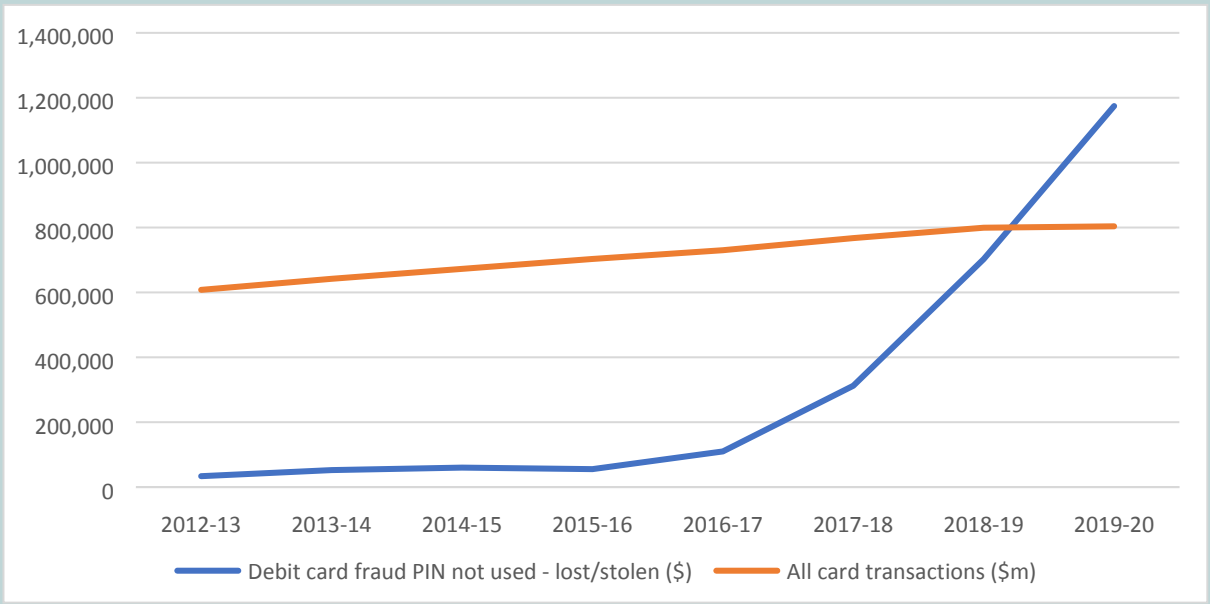
Figure 1: Cumulative number and value of COVID-19 scams reported to Scamwatch, 1 March 2020 to 30 May 2021



Note: Number and value of reports made to Scamwatch in the calendar years preceding the months beginning 1 March 2020 to 30 May 2021 in Australian dollars

Source: ACCC unpublished data, 2021

Figure 2: Value of debit card frauds involving lost and stolen cards in which PINs were not used, 2012-20 ($)



Source: AusPayNet 2021

Table 1. United Kingdom fraud losses (£stg) by fraud type, 2011-2020

Fraud Type	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	% Change 19/20
Remote Purchase (CNP)	£221.0	£247.3	£301.0	£331.5	£398.4	£432.3	£408.4	£506.4	£470.2	£452.6	-4%
Of which e-commerce	£139.6	£140.2	£190.1	£219.1	£261.5	£310.3	£310.4	£394.2	£360.5	£376.5	4%
Counterfeit	£36.1	£42.3	£43.3	£47.8	£45.7	£36.9	£24.2	£16.3	£12.8	£8.7	-32%
Lost and Stolen	£50.1	£55.4	£58.9	£59.7	£74.1	£96.3	£92.9	£95.1	£94.8	£78.9	-17%
Card ID Theft	£22.5	£32.6	£36.7	£30.0	£38.2	£40.0	£29.8	£47.3	£37.7	£29.7	-21%
Card non-receipt	£11.3	£12.8	£10.4	£10.1	£11.7	£12.5	£10.2	£6.3	£5.2	£4.4	-15%
Total	**£341.0**	**£390.4**	**£450.2**	**£479.0**	**£568.1**	**£618.1**	**£565.4**	**£671.4**	**£620.6**	**£574.2**	**-7%**
UK	£260.9	£288.4	£328.2	£328.7	£379.7	£417.9	£407.5	£496.6	£449.9	£414.5	-8%
Fraud Abroad	£80.0	£102.0	£122.0	£150.3	£188.4	£200.1	£158.0	£174.8	£170.7	£159.7	-6%