Australian Government
Australian Institute of Criminology

AIC reports
Research Report 19

Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19

Michael Levi
Russell G Smith

ISSN (Online) 2206-7280
ISBN 978 1 922478 11 5 (Online)

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to double-blind peer review.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Boxes

Acknowledgements

Research assistance with the Australian content was provided by Christie Franks, Cameron Long and Coen Teunissen and the staff of the Australian Institute of Criminology's JV Barry Library.

Abstract

This report seeks to draw out the common characteristics of frauds associated with pandemics, and to identify any risks unique to pandemics and financial crises, beginning with the Spanish flu pandemic of 1918, as the closest to COVID-19 in the modern era. It summarises the general influence of the internet or remote intrusions on contemporary frauds and allied corporate/organised crimes against individuals, businesses and government, using plausibly reliable data from Australia and the United Kingdom as indicative of more general trends. The report identifies some novel crime types and methodologies arising during the COVID-19 pandemic of 2020 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. The report notes that many frauds occur whatever the state of the economy, but that some specific frauds occur during pandemics, especially online fraud. Similarly, some previously occurring frauds are revealed by economic crises, while frauds arising from and causing insolvencies are stimulated by economic crises. The report concludes with a discussion of the policy implications for prevention, resilience and for private and public policing and criminal justice in Australia. It stresses the need for plans for future pandemics and economic crises to include provisions for better early monitoring and control of fraud and procurement corruption.

Executive summary

This review begins with a very brief rationale for the selection of particular pandemics and other major social and economic crises since the First World War, beginning with the Spanish flu pandemic of 1918, as the crisis most similar to the COVID-19 pandemic in the modern era, and including the influenza pandemics of 1957 and 1968. It includes other major economic shocks such as the Great Depression of the 1930s, the Asian financial crisis of 1997, and the global financial crisis of 2008–09. The study seeks to draw out the common characteristics of frauds associated with pandemics, and to identify any risks unique to pandemics and financial crises, and to assess the general influence of the internet and remote intrusions on contemporary frauds and allied corporate or organised crimes against individuals, businesses and government, using data from Australia and the United Kingdom as indicative of more general trends.

Some trend analysis using officially recorded fraud data from the United Kingdom and Australia—and any recent data on payment card fraud or from business surveys—will chart how recorded crime changed following previous shocks and pandemics. Where possible, these crime trends are mapped to business activity levels. The report explores what we can learn about the responses of individuals and organised crime to specific initiatives and other activities. These include: social distancing, loan/mortgage repayment freezes, pensioner cash payments, limiting cash payments in favour of contactless payments, profiteering from the sale of health products, social welfare fraud, identity misuse, IT fraud arising from data manipulation and phone plans, corporate fraud or phoenixing, payroll fraud, employee wage theft or dishonest underpayment of staff, consumer scams, insurance fraud and contractual dishonesty in non-repayment of deposits on bookings or failure to repay government-guaranteed loans.

We seek to identify any novel crime types or methodologies not seen during previous pandemics that have arisen during the COVID-19 pandemic, perhaps because of specific economic and public health measures. By necessity, this will not be an extensive review of those issues, but will canvass the problems and solutions in a concise and practical way. Many frauds occur regardless of health or economic crises, but some specific frauds, especially online frauds, occur in response to the circumstances involving pandemics. Similarly, some frauds that were previously occurring are revealed by economic crises, while frauds arising from insolvencies are stimulated by economic crises. Some substantial procurement and loans frauds against government are likely outcomes of pressures to buy health products rapidly and to encourage banks to lend to businesses.

The report reviews existing projections of changes in online and offline economic crimes. It analyses how fraud and economic crime may plausibly change by June 2022 as a result of the coronavirus pandemic, via expected socio-economic impacts and changes in motivation, opportunities and guardianship capabilities. It concludes with a discussion of the policy implications for prevention, for building resilience and for private and public policing and criminal justice responses, focusing on Australia. Whatever the need for improvement of policing and prosecution to enhance legitimacy in the eyes of the public and to deter crime, the report stresses that plans for future pandemics and economic crises must include provisions for better monitoring and control of fraud. The faster that loans are monitored and controlled, the less will be lost to fraud. To achieve this, greater transparency and accountability are needed in the implementation of government pandemic response initiatives.

Introduction

There are many and diverse forms of economic crime, some of which have a prima facie connection to pandemics and economic crises and others of which may not. The plausible direction of causality is important to consider. Do frauds exacerbate or even lead to economic crises? Do such crises generate opportunities for fraud, and do they always do so, or are these risks connected to specific initiatives developed in response to crises? Are the offenders in these contexts the same ones who commit frauds at other times, or are there new entrants into the criminal markets? How does the behaviour of past and potential victims—whether individual, corporate or governmental—change during such times? Or are pandemics and economic crises largely or even only a hook on which to hang scams that might well have been perpetrated anyway? Is the health and economic crisis of 2020 so unlike previous ones that it is foolish to seek parallels, which are likely to be modest at best? What lessons have been learned, or not learned, from previous crises?

Contemporary discussions invariably show some awareness of the problem of non-reporting as well as non-prosecution of fraud. Existing data need to be considered within the context of the elapsed time to detection (which can be infinite if undetected or misidentified as 'not fraud'), and to formal intervention, whether regulatory or criminal; this will vary by type. Large internal frauds and corruption usually take longer to surface and also to investigate and prosecute. Since we will be reviewing frauds over the last century, focusing on the United Kingdom and Australia, there have been many changes in reporting, recording and processing them, in addition to the technological changes in fraud commission, prevention and pursuit as we move from the telegraph to cyberspace and cryptocurrencies as mechanisms for funds transmission, and from the biblical apple to Apple as mechanisms of temptation.

There are a number of perspectives from which this could be analysed:

- examining a set of 'known frauds' by subtype and seeing whether their commission and their exposure are related to pandemics and economic crises.
- examining periods of pandemic and economic crises and analysing what sorts of frauds and other economic crimes are known to have occurred then, to try to calculate some equivalent of 'excess deaths' for economic crimes.

It is important to consider if changes in monitoring and policing or regulatory responses might be responsible for any changes in official data, and therefore whether changes in reported or recorded 'fraud rates' may be an artefact of increased or reduced reporting and willingness to act rather than reflecting a real change in fraudulent behaviour.

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 & Spalding LLP 2020). In the United Kingdom, the 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 (eg 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 'gouging' (see, for example, the fascinating discussion of the criteria for 'profiteering' in the parliamentary debate on what became the UK *Profiteering Act 1919*; House of Commons 1919).

Also relevant to the scope of illegal activity during pandemics is the question of whether or not the category of fraud or 'product counterfeiting' includes homeopathic and prescription 'cures' for which there is no good scientific evidence according to the standards of the day. When, for example, do scientifically unproven claims about the alleviating effect of 'healthy products' become deceptions sufficient to be included in the category of economic crimes, and does this classification as fraud require proof of intent or recklessness? In the United States, one organisation reviewed the research on vaccines and drugs used in previous pandemics, before praising the preventative qualities of honey, noting that 'natural products can only ease the symptoms and support your own immune system' and that readers should 'avoid coronavirus scams!' (Healthy with Honey 2020). Crime features only intermittently in classical accounts of the causes of economic crises, and barely at all in accounts of pandemics (eg Zinsser 2000). Although corruption in international aid to the Global South commonly features in the development literature, it is only intermittently linked to pandemics or indeed to economic crises. In his analysis of the Black Death in Naples in 1656, Snowden refers to:

> …the breakdown of law and order and the collapse of every public service including instances of fraud and profiteering: astrologers peddled advice and prognostications, charlatans hawked their nostrums, and healers of every description charged astonishing sums for practising their arts. (Snowden 2020: 59–60)

None of the major books on the Spanish flu epidemic discusses frauds, and corruption is mentioned only in the metaphorical or spiritual sense. Consideration will be given to the evidence on black marketeering and other crimes in wartime later, but apart from Clinard's (1952) own work, criminologists have not been greatly interested in either black marketeering or pandemics, perhaps because, until the COVID-19 one, pandemics have been more salient to Asian countries, where white-collar crime research is less developed, but also perhaps because white-collar criminologists have been more focused on misconduct by or against big corporations by senior insiders. For example, white-collar crime research has tended to focus on big corporate price gouging rather than scams against government or individuals by organised criminals.

Economic crime is a mixture of different sorts of high- and low-volume crimes with different probabilities of being reported to the authorities and being acted upon. But some insights may be gleaned from the framework for the dynamics of crime developed in one study of the impact of recessions on illegal drug use (Nagelhout et al. 2017) and another cautionary study on the impact of COVID-19 on drug markets (Giommoni 2020). We would anticipate that different forms of economic crime might have different rates of change, with or without the health and economic crises and the large economic stimulus packages that are far more a feature of the COVID-19 crisis than of earlier pandemics. But this is not simply a question of financial losses: the emotional and financial impacts of fraud are affected by their affordability to those who suffer harms, and they include the impact on trust and confidence in the authorities to prevent fraud and to pursue justice. Finally, the report examines whether anything has been learned, or reasonably could be learned, from the economic crime and crime control responses that followed previous pandemics, economic shocks and crises.

Economic crimes and pandemics

We begin our analysis with pandemics in the modern era:

- 'Spanish flu' 1918–19 (misleadingly named because during the First World War Spain was neutral and did not censor its press, leading to an incorrect perception that Spain was the origin);
- Asian flu 1957–58;
- Hong Kong flu A (H3N2) 1968;
- swine flu A (H1N1), 2009–10; and
- COVID-19, which was first identified in Wuhan, China.

Resource and time constraints lead us to focus primarily on Australia and the United Kingdom as the objects of study: in practice, this means a focus on Spanish flu and COVID-19 because the other pandemics hit the above jurisdictions much less hard.

Little attention in the Global North was given to economic crimes during pandemics before COVID-19, though there have been efforts during each pandemic to discredit fake cures, which appear to have accelerated as social media and anti-government scepticism have generated misinformation and commentaries about health risks. For example, genuine Chinese water-snake oil introduced into the United States by Chinese labourers during the nineteenth century contained high levels of omega-3, which can reduce inflammation (Graber 2007). However, many products claiming to be snake oil contained none, and this led to occasional prosecutions and to the popularity of the phrase 'snake oil salesman', meaning someone selling over-hyped items (Graber 2007).

The major books and journal articles on Spanish flu do not mention fraud or corruption (except as metaphors), focusing understandably on the dynamics of the pandemic. Among the few Spanish flu era media crime stories is that of 'Slick Julia' Lyons, who, despite having no real medical qualifications, signed on to the home nursing registry in Chicago and fleeced her patients, in the end being sentenced to one to 10 years imprisonment (Shafer 2020). Even in that case, the fraudulent qualifications were more of a route to theft than 'real' fraud as a crime technique. Spanish flu fears also generated a rise in seances and spiritualism in the United States (Daugherty 2020). 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).

Research into the Spanish flu period shows some commentary on the role of otherwise legitimate corporations and shyster firms in making false claims that their products could prevent and alleviate Spanish flu. This commentary occurred in the United Kingdom, in what is now the Irish Republic, and in the United States, where the public were advised, among other things, to 'eat more onions' (Arnold 2018). 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).

In the United States, numerous advertisements appeared for allegedly health-giving products and also for questionable paid learning systems for nurse training, which may or may not have been a good investment (see, for example, Wall Street Journal 2020 and Vollet 2020). There is no reason to suppose that any of the products advertised were in any way harmful to users. They are, however, indicative of the changes that have gone on in the past century in what is acceptable and also what is regulated when advertising health benefits. Vick's VapoRub, for example, promoted itself during the Spanish flu era with adverts that vastly boosted its sales. One advertisement, for example, states: 'How to use Vick's VapoRub in treating Spanish Influenza: The influenza germs attack the lining of the air passages. When VapoRub is applied over throat and chest the medicated vapors loosen the phlegm, open the air passages and stimulate the mucous membrane to throw off the germs' (UNC Libraries 2020; see also Modern Mississauga 2020). Some of the firms included testimonials from soldiers or doctors about the efficacy of lotions such as Veno's in preventing Spanish flu.

In Ireland, Oxo and Bovril advertised their value in fighting off Spanish flu, though they were careful not to advertise themselves as a medicine, so this is not fraud. However, if the advertising agencies had even suggested it, regulators today would likely require the adverts to be taken down (Marsh 2019). Other firms were less careful. An unduly positive sense of protection against Spanish flu would have been generated by the cognitive associations in the commercials (see Marsh 2019).

Shore (2015) does discuss fraud and organised crime in the United Kingdom up to the end of the 1920s, but nothing in her research suggests that Spanish flu or fear of it was used as part of these frauds or organised crime activities.

Pandemics before 2020 did not lead either to 'moral panics' about fraud or corruption or to noticeably unusual levels of fraud in Australia, the United Kingdom or the United States, though they may have done in Asia, where the reporting is harder to access and the crime statistics are even less valid or reliable. The *New York Times* contains no articles on frauds or scams connected to 20th- or 21st-century pandemics prior to 2008, and only one in 2009, but some local US papers warned of scams and the US Food and Drug Administration and the UK government did warn especially about fake cures and counterfeit drugs (FINRA 2020). Then, but less visibly or commonly than now, there were claims that the pandemics themselves were illusions or what would now be termed 'fake news'. In 2005 US investors were warned about stocks being promoted with false claims that companies were poised to benefit from vaccines (FINRA 2020).

Many false claims were made during the swine flu pandemic of 2009–10, leading federal officials 'to send warning letters to promoters of more than 140 swine flu-related products, including well-known alternative medicine advocate Dr Andrew Weil for his "Immune Support Formula"' (Marchione 2009). These included outright scams involving fake Tamiflu and health products like the 'Photon Genie', whose energy waves allegedly eliminated swine flu, and otherwise legitimate businesses who sought to boost sales with recklessly optimistic or actively deceptive claims. The Food and Drug Administration stated that swine flu scams appeared soon after swine flu itself arrived; this later happened with COVID-19 scams, and indeed with other events. In Australia, the swine flu pandemic saw a large increase in online scammers seeking to profit from the health crisis. Billions of spam emails containing malware were reported, including offers of virus information, discount pharmaceuticals and survival kits that were used to extract personal identification information and money from Australians (Australian Competition and Consumer Commission (ACCC) 2009).

During the swine flu epidemic in China in 2018, some Chinese gangs slaughtered pigs, claiming that the pigs had swine flu, and then forced African farmers to sell pork to them at a reduced price because of the health scare about pork they themselves had generated by playing upon existing scares (Daly 2019). In a very different sort of case, an analyst from the Swiss investment bank UBS referred to 'Chinese pigs' in a report on pork trends, which led to a Chinese backlash against the bank, showing the risks attached to the use of language, especially when inflamed by commercial rivals (Weinland, Jenkins & Crow 2019).

This might be described as 'moral panic for profit'. Although there is little discussion of pandemics and fraud, there is a small amount of literature on fraud and corruption following (and sometimes causing) disasters. Frailing and Harper (2017) pull together many of these case studies and examples in the United States, breaking them up into individual contractor fraud, price gouging and profiteering, disaster benefit fraud, and corruption; and corporate disaster fraud, including frauds by insurance companies, as liabilities are shifted onto the government or corporations.

However, the authors note that they focus on the latter phases of disaster, which they assert is when crimes of fraud tend to occur. If their work was more international in focus, they might have considered European and developing countries, where corruption and fraud in public contracting has led to the collapse of bridges, roads et cetera. However, none of this relates particularly to pandemics, so we will not discuss this further, except to note that more Australian and UK government payouts were made to businesses and individuals during the 2020 pandemic than in any other historical disaster. These government responses were also made at a time when staffing in agencies supplying funds and controlling fraud was particularly constrained by the personnel contracting the virus and by having to work from home.

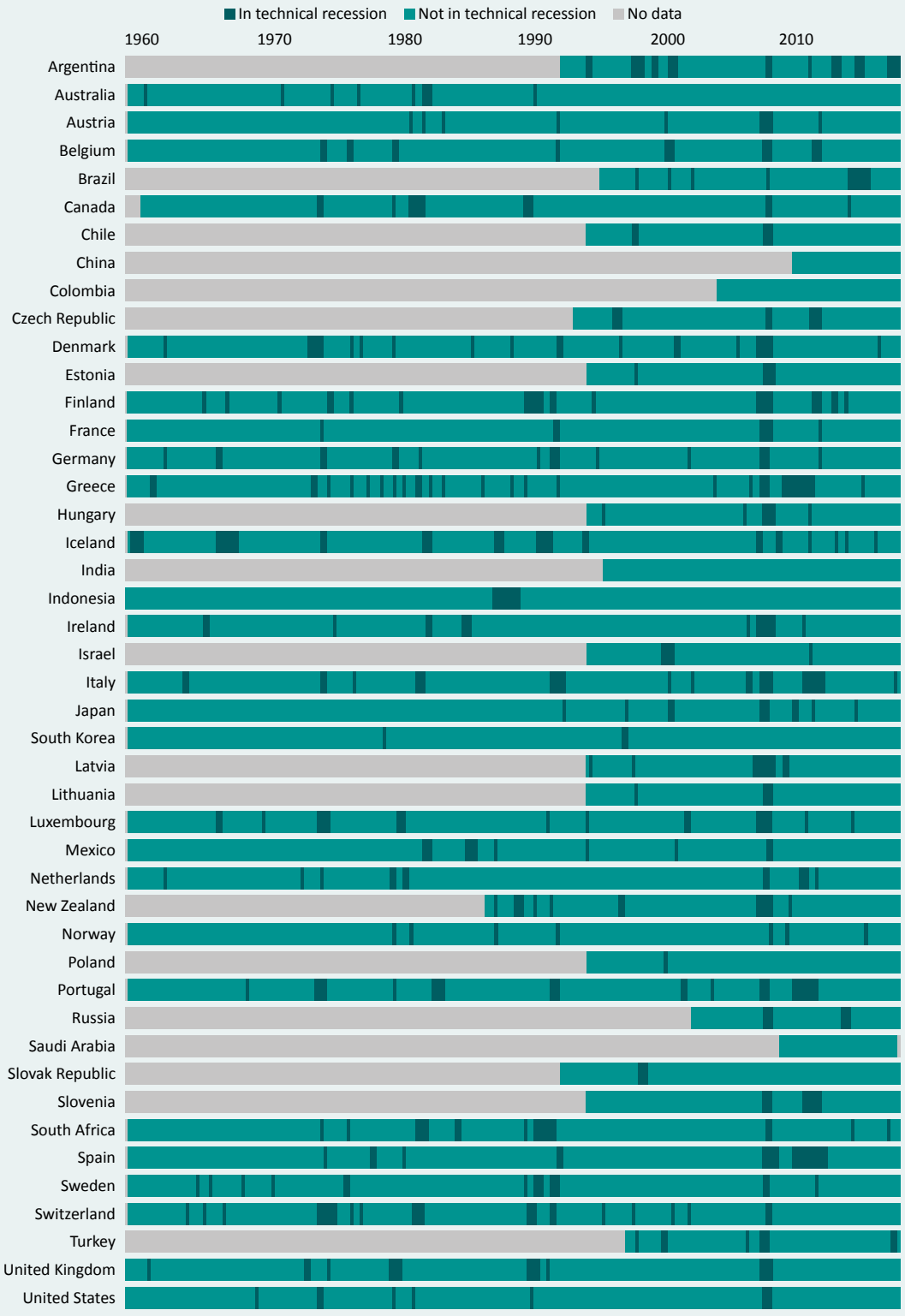
Public warnings about scams have become more proactive in 2020 in Australia, the United Kingdom and the United States, though there remain arguments about the effectiveness of these warning techniques (Fair 2020; Federal Trade Commission 2020). These arguments are out of scope for this study. Indeed, it seems reasonable to suggest that the COVID-19 pandemic represents the first time that there has been a systematic approach (at least in the anglophone global north) to combating health and financial scams during a pandemic, or even during an epidemic, fuelled by more general contemporary concerns about the impact of the internet and social media on fraud affecting the general public (and politics). When considering this, it may be helpful to think of these educational efforts as demarcated by public warnings about consumer and investment scams from the financial sector (eg FINRA 2020), government (eg www.scamwatch.gov.au), non-profit bodies, and even some social media companies (eg Google's https://scamspotter.org/). These approaches have also included efforts within the public sector to reduce fraud against government expenditure; and advice from financial consultancies and government to the business sector aimed at reducing fraud risks from changes in the organisation of business in the short and longer term transition to working from home.

To date, none of this public advice relates directly to reducing the risk of fraud committed by senior executives. It is important to place COVID-19 scams in perspective. A huge number of elite, blue collar and 'organised crime' frauds go on independently, generated by a wide range of opportunities and motivations. Pandemics alter the shape of some of these opportunities and pressures on individuals, but they do not dominate fraud or other economic crimes.

Crime and economic crises

The literature on fraud and economic crises is more substantial than that on pandemics, but is still modest and patchy. The International Monetary Fund defines a global economic crisis as a decline in real per-capita world gross domestic product, in the context of changes in other global macro-economic indicators. Those indicators include industrial production, trade, capital flows, oil consumption and unemployment. By that definition, prior to 2019, there have been four global recessions since World War II: in 1975, 1982, 1991 and 2009, of which 2009 was by far the greatest and most widespread (Davis 2009). National recessions are more common (for the wealthier OECD countries, see Figure 1).

Figure 1: Technical recessions, 1960–2019



Source: Kiersz 2019 and OECD 2020

The magisterial account of 800 years of financial follies by Reinhart and Rogoff (2009) contains no references at all to fraud, scams, misconduct or crime in its entire 512 pages, though a 4th-century swindle is mentioned briefly. Aliber and Kindleberger (2015) frequently mention them in the seventh edition of their book *Manias, panics, and crashes*, which has a whole chapter on frauds (ch 7) and deals with 10 financial bubbles (2015: 18), seven of which fall within the period of study (see Box 1).

Box 1: Financial bubbles throughout history	
1	The Dutch tulip bubble 1636
2	The South Sea bubble 1720
3	The Mississippi bubble 1720
4	The stock price bubble 1927–29
5	The surge in bank loans to Mexico and other developing countries in the 1970s
6	The bubble in real estate and stocks in Japan 1985–89
7	The 1985–89 bubble in real estate and stocks in Finland, Norway and Sweden
8	The bubble in real estate and stocks in Thailand, Malaysia, Indonesia and several other Asian countries 1992–97 and the surge in foreign investment in Mexico 1990–94
9	The bubble in over-the-counter stocks in the United States 1995–2000
10	The real estate bubble in the United States, Britain, Spain, Ireland and Iceland between 2002 and 2007

Source: Aliber & Kindleberger (2015)

The manias and banking crises in the nineteenth century often occurred after a period of extended investment in infrastructure such as canals and railroads. Banking crises were frequent between 1920 and 1940. The percentage increases in stock prices between 1980 and 2020 were larger than in earlier times, and five of the 10 manias in Box 1 occurred in this period. Sharp increases in prices of real estate and of stocks have often occurred together, perhaps because many listed companies own large amounts of real estate. But Ponzi schemes and other 'bubble' business promoters appear to use as a rationale for their promotions both the prospect of being in on the ground floor of booming economic activity and (as in the most recent years, even preceding the COVID period) the need to beat low interest rates. Aliber and Kindleberger (2015: 29–30) state:

> Crashes and panics are often precipitated by the revelation of some misfeasance, malfeasance or malversation (the corruption of officials) that occurred during the mania. One inference is that the swindles are a response to the appetite for wealth (or plain greed) stimulated by the boom; the Smiths want to keep up with the Joneses and some Smiths engage in fraudulent behavior to do so. As the monetary system gets stretched, institutions lose liquidity and as unsuccessful swindles seem about to be revealed, the temptation to take the money and run becomes irresistible.

However, as we shall see, this tells only part of the story, reflecting their focus on macro-economic factors in crises and a limited range of frauds that they consider relevant to that narrative, which largely excludes outright planned scams and volume frauds. Chapter 7 of their book is a history of financial scandals at various periods, but none of the examples cited mention pandemics, and the main theme is that fraud goes up during boom times, when people want to share in the benefits of growing profits. Some of the most damaging corporate frauds get shaken out in recessions. More often, however, those corporate deceptions that fall short of outright Ponzi schemes happen because corporate acquisitions have to rise faster than market expectations to sustain stock prices, and the schemers run out of time since under-priced businesses are no longer available to buy to boost share prices. This is what occurred in the case of Enron (Fox 2003). Ponzi schemes are inevitably self-liquidating, though some like Bernie Madoff's may last for years (see Balleisen 2017).

Van Driel (2019) gives a good conceptual overview of anglophone historians' work on fraud. There has been far more work on fraud in Victorian Britain than on any other time, and although histories of the United States often contain colourful accounts of the depredations of the 'Robber Barons' during the nineteenth century, this is not linked in the literature to any pandemic (other than greed!) nor to any macro-economic crises. Shore (2015) does discuss fraud and organised crime in the United Kingdom up to the end of the 1920s, but economic crises make an appearance only in influencing the media and social construction of the problem as threatening 'Englishness' in the post-World War I period. In his extensive classic *Social aspects of crime between the wars*, Mannheim (1940) discusses only five instances of fraud, which, he states, more closely than other crime 'follows the zigzag course of the economy, political and social life of the country, although its relation to the business cycle may differ from that of larceny' (1940: 118). He mentions charity frauds, and also that whereas most frauds and corruption in Germany require the connivance of public officials, British frauds do not. He draws attention to share-pushing frauds, to drawing unemployment benefits while working, to railway fare evasion frauds, and to bankruptcy frauds as rare examples of recidivist swindlers. However, no particular link is made to the Great Depression or to other economic booms or busts, which does not mean that there is no link: the absence of evidence is not evidence of absence.

Maurer's (2000) classic ethnographic text *The big con* (originally published in 1940) discusses extensively frauds in the early part of the twenty-first century, though not with any focus on the Great Depression or its effects on these cons. A short introduction by Sante (2000) to the republished edition of *The big con* notes that the 'golden age of the big con' was from the turn of the century to the Great Depression, with its peak occurring roughly 1914–1923, being a period of rising affluence and socio-economic mobility in the American middle class. Sante (2000) plausibly asserts that this led people to have confidence in their own perspicacity and enhanced their vulnerability to fraud, a view consistent with more recent work on the social psychology of deception (eg Cialdini 2009). Houlbrook's (2016) absorbing study of post-World War I 'gentleman crook' Netley Lucas shows how he simulated the dress style and provenance of a gentleman and former naval officer to leave a trail of debts, and even his imprisonment and criminal autobiography appeared not to dent his credibility; indeed, it added to his apparent authenticity. However, this might be interpreted better as a way of imitating credit-worthiness in the (later) manner of 'Catch me if you can' Frank Abagnale, and there is nothing to connect his conduct to either Spanish flu or the recession that started in the late 1920s.

More serious is the argument over the role of fraud in stimulating or causing the Great Depression. Blinder (2014) defensibly prefers to call 'near-fraud' the conflicts of interest and the manipulations of profitability and securities that precipitated the Wall Street crash of 1929 and which, via national protectionist policies, generated economic crises in Europe and elsewhere. Other commentators (and the Pecora Commission established in the 1930s to investigate the causes) are less hesitant in labelling the conduct as fraud (Balleisen 2017). Given that no-one was jailed for the malefactions (though some were jailed for other fraudulent conduct), it might be more accurate to state that the (mis)conduct was regulated or criminalised as part of the New Deal reforms in the mid-1930s. So it might well have been fraud had it occurred later but was not (criminal) fraud at the time.

A hypothesis that the Great Depression caused fraud would need to examine when the misconduct began, to test the proposition that it was caused by the Depression rather than that the Depression revealed what had been going on before. As at present, many 'short cons' may not lead to prosecution but they appear rapidly after commission, whereas other frauds take years to be completed and dealt with. Credit for individuals for consumer purchases or even for mortgages barely existed for the masses in the 1920s and 1930s, but the normal effect of recessions is to make credit harder to obtain. This means that many people must deceive to get credit, making them technically fraudsters even if they were not what Levi (2008) terms 'pre-planned' fraudsters. Telling lies to get fresh credit or to delay repayment would be 'slippery slope fraud', and that may have been the characteristic feature of most business and individual fraud in the 1930s. Other economic crises prior to 2008 were less global. Some authors include the fraud-rich 'dotcom' bubble, which mainly affected the United States and Europe, though it affected some international investors: too complex and large a topic for this account. This bubble certainly led to an accentuation of frauds, as businesses piled on deceptions in order to keep in business.

Economic crimes and the 'black market'

There is limited literature on the black market economy in the United Kingdom (Ellis 2018; Roodhouse 2013; Smithies 1982) and even less on that of Australia (Grabosky 1977; Treasury 2017). Smithies does mention the theft of gas masks, but not in the context of our contemporary concern with personal protective equipment (PPE) but for tax reasons: pouring petrol, stolen from military storage dumps, through a gas mask to filter out the distinctive coloured dye put in to deter tax-evaded resale. One notes the marginal, vicarious involvement of thousands of otherwise law-abiding citizens who in a time of acute scarcity were reluctant to identify criminal suppliers if this meant the supply drying up.

Roodhouse's (2013) analysis examines, among other things, the way in which officials calculated a fair share, a fair price, and a fair profit, and—relevant to contemporary perceptions of price 'gouging'—how official understanding of fair shares clashed with popular notions of distributive justice. Discussing the four-week imprisonment of composer and actor Ivor Novello for cheating war rationing of petrol with the assistance of a member of his fan club, and the economic analysis of black marketeering, Roodhouse (2013: 6) critiques economists' approach, noting that 'neither Boulding nor Becker acknowledged that the emotional content of social norms governing the exchange, distribution, and use of resources makes cold calculation difficult if not impossible'.

It should, however, be noted that cold calculation is precisely what is normally applied to medical interventions to judge cost-effectiveness. The COVID-19 pandemic has shown how, at times, this model is overridden by the politics of health care: COVID-19 deaths appear to be weighted far more heavily than other deaths (and medical help foregone) in the political cost–benefit analysis. Roodhouse (2013) goes on to stress the high tolerance of black marketeering for both barter and low-profit money among the middle as well as working classes, but the intolerance of professional criminal price gouging of gangsters. This theme is taken up by Farrall and Karstedt (2020) in their analysis of middle-class offending and attitudes to offending, mostly in Europe, in the twenty-first century.

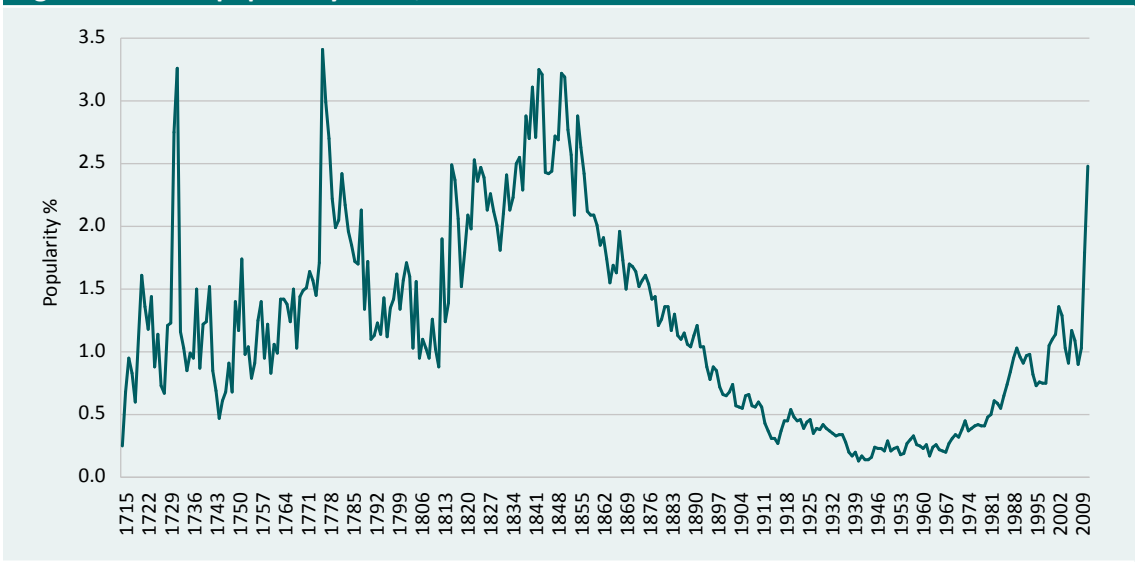
In addition to the black market, many other wartime activities offered scope for the unscrupulous (Ellis 2018). For example, the massive amount of civil defence work commissioned was ripe for corruption and fraud: in West London, a contractor conspired with the London Hammersmith clerk of works to falsely certify air-raid shelters as sound when they had been shoddily built and fraudulently expensed and were unfit for purpose. People died who should have been safe from the bombs, and manslaughter prosecutions followed. Some doctors profited from a popular scam of providing false military exemption certificates to those who did not wish to fight: a broader theme of relevance to some contemporary politicians. Dr William Sutton of Stepney (East London) would freely issue such exemptions for half a crown without even bothering to see the 'patients'. He went to jail and his name was removed from the Register of Medical Practitioners in May 1943, although it was restored after 54 months.

Smith (1994) recorded the large increase in disciplinary cases coming before the General Medical Council in which medical practitioners gave false certificates allowing their 'patients' to avoid military service during the Second World War. Cases of fraud involving doctors also increased during and following the wars. This is the kind of fraud that might be picked up with modern data analysis, if issuers of exemptions or other 'enablers' were included in the datasets.

Fraud reported in the media

Toms (2019) provides evidence on the patterns of fraudulent behaviour over extended periods of time, based on content analysis of contemporary news sources in the United Kingdom (1715–2009) and the United States (1850–2009) and a database of 221 British corporate scandals (1800–2009). This analysis is very useful and competent, but his chosen focus is on the implications for auditing, and most 'garden variety' frauds are of little interest to auditors or to political economists, and therefore fall beyond Toms' purview. Furthermore, the analysis of financial scandals understandably shows little interest in the selective nature of media publicity, which focuses on 'newsworthy' material which touches either business or populist local and national concerns (Levi 2006, 2008), omitting duller cases which do not stimulate the interest of the public to read or view, or (important to contemporary media) generate online advertising revenue (Figure 2).

Figure 2: 'Fraud' popularity index, 1715–2009

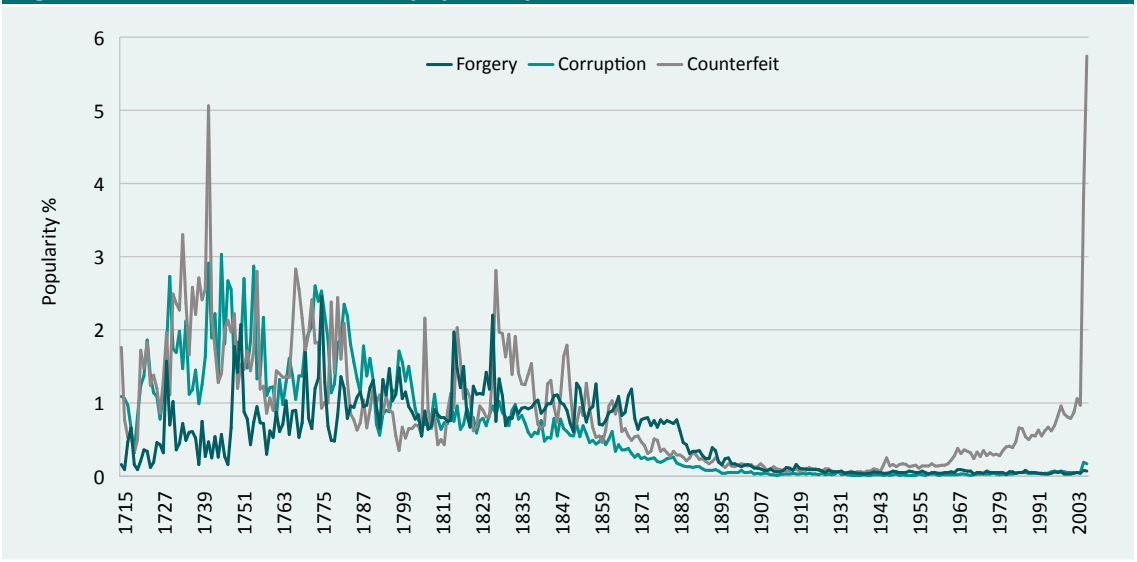


Note: Popularity % is the number of documents featuring 'fraud' divided by all relevant documents, where a relevant document is a news story published in the 'News', 'Business News' or 'Opinion and Editorial' section of a newspaper/periodical as defined by the Cengage database

Source: Calculated by Toms (2019) from Gale Cengage online database of British newspapers

Figure 3 presents data on generic financial crime for 1715–2009 calculated from the Gale Cengage online database of British newspapers.

Figure 3: Generic financial crime popularity index, 1715–2009



Note: Popularity % for each term is number of documents featuring 'forgery', 'corruption' or 'counterfeit' divided by all relevant documents, where a relevant document is a news story published in the 'News', 'Business News' or 'Opinion and Editorial' section of a newspaper/periodical as defined by the Cengage database

Source: Calculated by Toms (2019) from the Gale Cengage online database of British newspapers

Tooze (2019) gives a much broader and deeper account of economic crises than authors discussed hitherto, though fraud does not appear in it. Overall it is clear from the broader historical literature that fraud is very seldom if ever macro-economically significant (in the International Monetary Fund's sense of that term). Widespread mortgage fraud in the United States came closest, with financial instruments precipitating the 2008 financial crisis, even if almost no-one in elite financial circles in any country was ever prosecuted for it. The label of 'fraud' was firmly resisted by politicians as well as by businesspeople, who preferred to deal pragmatically with the economic problems without the inconvenient obstacle of moral hazard or crime getting in the way (Levi 2009). However, though the scale of the mortgage fraud and the sheer volume of over-valued synthetic finance on the back of it had an impact on the crash, the sudden loss of credit shook out the mortgage frauds involving the 'self-declared income' of those who were not legally eligible for the large loans they received. They had been encouraged to falsify their incomes by brokers (who often completed the application forms for them, sometimes without their detailed knowledge), and the securitisation process through law firms and investment banks systematically over-graded the value of the loan books thus falsified, with disastrous consequences once the Lehman Brothers collapse pricked the bubble (Balleisen 2017; Fligstein & Roehrkasse 2016; Tett 2009; Tooze 2019). So as with the Great Depression of the 1930s, although the serious financial misconduct of major market actors led to great socio-economic harm, the crime and criminal justice statistics show that identified fraud rates were low and that the frauds were mostly committed by social outsiders.

Some frauds whose commission long preceded economic crises are brought into victim and/or public consciousness as a result of the credit squeeze. Some 'organised criminals' (an ambiguous term of art) may be drawn into greater confidence in making fraud participation offers to insiders or blackmailing them because of the insider's inability to repay debts and because they believe that people are more corruptible at times of economic stress. Some fraud opportunities linked to workplaces will be reduced because if people motivated to defraud have lost their jobs, they can no longer commit internal frauds. But in other cases where opportunities remain, temptations are greater because of the desire not to lose lifestyle and social status.

Levi (2008) categorises fraud as pre-planned fraud, intermediate fraud (starts off honest and consciously turns to fraud), and slippery-slope fraud (tells lies to continue trading, in the unrealistic hope that things will turn around). Using this typology, there have been both extra and reduced risks of motivation, opportunity, and capable guardianship. The net effect of these changes is difficult to determine, and most fraud data—other than plastic card fraud—are too dependent on changing probabilities of recognition, reporting and recording to enable confident inferences about trends to be drawn. It seems plausible that more slippery-slope insolvency frauds occur in times of recession, as some company directors and professionals seek to protect income and wealth from the economic consequences of the downturn. There is no evidence that the global financial crisis of 2008–09 had a major impact on increasing the cost or levels of fraud overall in the areas about which we have the best knowledge: Australia, the United Kingdom and the United States. However, the scale of the public expenditure stimulus schemes of 2020 present particular risks of fraud that, as far as is known, have not been present to the same extent in earlier pandemics and economic crises. The 2020 pandemic also created opportunities for other types of financial misconduct and suspicions thereof—for example, where contracts were entered into for the supply of PPE with companies without a demonstrated track record in fulfilling such obligations, leading sometimes to poor quality products, default and very high profits for intermediaries, as well as side-stepping genuine and competent firms. It also provoked concerns in the wider community about the ability of governments to minimise risks of procurement fraud and corruption in times of national emergencies.

Some arguably trivial points are worth stressing. To the extent that crimes are occupational, one must have an occupation in order to commit them: thus, though motivation to offend may rise during economic crises, opportunities to defraud may fall. To illustrate this, before their corporate collapses, fraudulent chief executives and dotcom bubble chiefs were able to allocate to the company expenditures that were in fact largely or wholly personal. Some of them went to jail for this, but not many. Economic pressures increase at times of crisis, but accountants, bankers and lawyers cannot readily manipulate clients' accounts or set up trust and other corporate secrecy vehicles if they no longer have jobs, though they (and anyone else) can make up imaginary firms and may have a pretext for fake corporate instructions to firms.

Unless constrained by culture, surveillance or anti-money laundering regulations, professionals in the same or another jurisdiction may be willing to take on the business. If others have confidence in them, entrepreneurs can develop new businesses that may generate new manipulative possibilities, but this would usually take longer at times of recession unless they tap into special government schemes.

At a lower status level of white-collar crimes, staff in call centres (whether physically located in the Global North or in anglophone India or Bangladesh) cannot so easily copy and extract personal data of account-holders if they are no longer employed in the call centres. If still employed, they may be more tempted to defraud if they consider that they may shortly become unemployed or that the company will show no loyalty towards them. The sudden furloughing of staff in call centres during the COVID-19 pandemic gave them little warning of their changed employment position, and UK police noted the decline in fake 'Microsoft engineer' calls attributed to 'rogue individuals or teams' in those call centres. This 'situational opportunity' model seems valid given that more people have been at home in the daytime to answer calls during the pandemic, so the available victim population is larger than normal. Financial and social pressures to offend may also be affected by fear of redundancy and peer group pressures, though threats from organised crime groups and ethnic/family loyalties may not be related to economic crises.

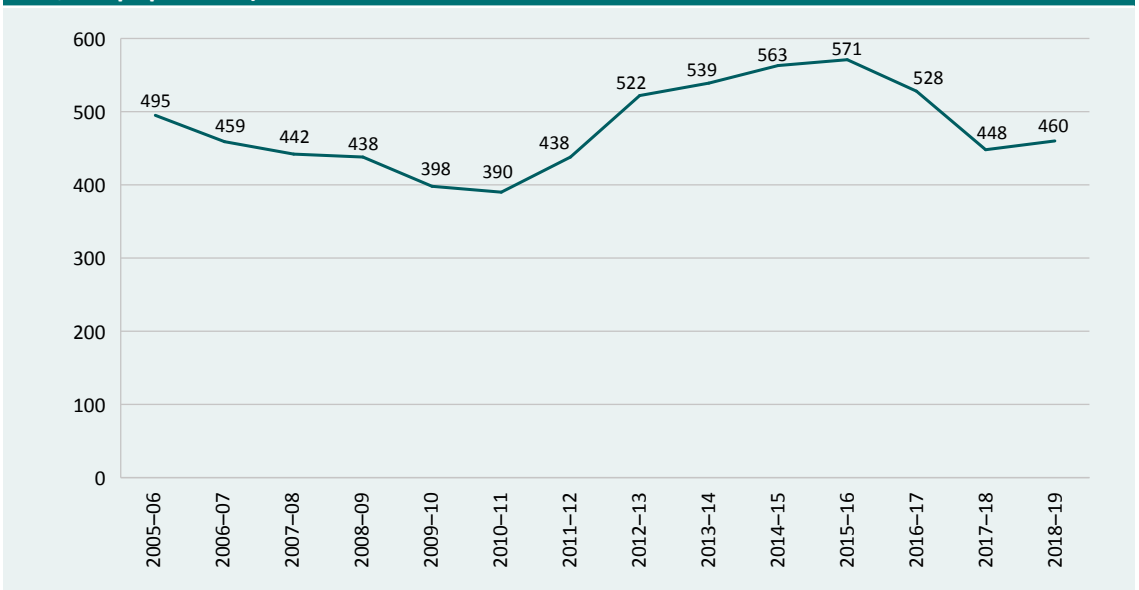
The ability of 'insiders' to offend may, however, be reduced by physical opportunity controls such as the absence of USB and CD drives on computers and rapid integrity checks. In addition, the miniaturisation of cameras and voice recorders on phones can assist data exfiltration for intellectual property crimes and the creation of scam 'sucker lists'. Under such circumstances, voluntary compliance via procedural legitimacy becomes much harder to achieve.

Rises in card-not-present payment card frauds are partly the product of increased opportunities and control weaknesses: they have little relationship to economic crises, though financial pressures may increase first-party frauds (by otherwise legitimate cardholders) or frauds by or in collaboration with merchants. The rise in mortgage frauds (Carswell & Bachtel 2009) and consumer/investment scams energised the regulatory process during the past decade, assisted by forensic linking software developments which make it easier proactively to search out connections between banking and insurance fraud networks. Since Ponzi investment pyramids rely on a high rate of incoming investments to sustain payouts, a fall in the rate of increase of investments or a reduction in the rate of reinvestment of imaginary profits causes them to collapse earlier. We should note also that, although there have already been some major corporate scandals during the present recession, the loss of confidence in growth and the rise in corporate short-sellers publicising their intensively researched (if often disputed) critiques of their target companies can serve to deflate the share prices and lead to (or sometimes follow) newspaper investigations that expose high level and serious corporate misconduct, including fraud and thefts of cryptocurrencies (see Poltz 2020 regarding the Wirecard prosecutions in Germany, which might not have happened without extensive *Financial Times* coverage despite attempted muzzling).

Australian perspectives on economic crises

Such historical accounts have focused on anglophone literature on the United Kingdom, United States and to a lesser extent Asia. Australia has not much interested them, being relatively unimportant to the world financial system (though important to this review and to people living there). However, financial journalist Trevor Sykes (1988, 1994, 2010) has written three lengthy books on the history of Australian corporate scandals, each showing how little businesspeople, politicians and regulators have learned from the previous crises, while academics such as Jones (2010) and Carnegie and O'Connell (2014) have dissected the issues. Levi and Smith (2011) examined the role that fraud played during and following the global financial crisis of 2008–09, and cited data on fraud offences recorded by police in Australia. Updated to 2019, Figure 4 shows that the rate of recorded fraud was declining prior to and during the global financial crisis but increased approximately two years later and continued to grow for a further five years. This reflects the time taken for cases to proceed through the courts, as well as the effects of the economic downturn on increasing the motivations for fraud offending. This has generated considerable concern in 2020, as the problems of adapting criminal courts to COVID-19 have led to massive delays in criminal justice (Transform Justice 2020).

Figure 4: Police recorded fraud and deception offences in Australia, 2005–19 (rate per 100,000 population)



Source: AIC statistical collection: recorded fraud data from police jurisdictions

Earlier Australian data on the rate of fraud, forgery and false pretences convictions in magistrates courts in New South Wales between 1880 and 1970 show troughs in convictions during war time, followed by increases shortly thereafter, as well as a marked increase during the Great Depression and following the Second World War (Figure 5). It should be noted that these data relate to lower court convictions in New South Wales only and would exclude major, serious and high-value matters. New South Wales was the only jurisdiction that had consistent fraud data during the years in question (see Mukherjee et al. 1988).

Figure 5: Fraud, forgery and false pretences convictions in New South Wales magistrates courts, 1880–1970 (rate per 100,000 population)

Note: Rates have been calculated on the basis of *Australian historical population statistics* (ABS 2008)
Source: Data are derived from Mukherjee et al. 1988: 278–80

For the purposes of this report, it is worth considering what the connection may be between these 'big economic crimes' and the smaller, blue-collar and white-collar ones and those committed by 'organised criminals' in the conventional sense of the term (see Levi & Soudijn 2020 for further discussion of the relationship between fraud and organised money laundering, and May & Bhardwa 2018 on fraud and organised crime groups in the UK). Cooper, Dacin and Palmer (2013) describe four domains of fraudulent behaviour: individual, firm, organisational field, and society at large. Gray, Frieder and Clark (2005: 41) argue that factors shown to be significant to financial bubbles include rapid economic and monetary expansion, the presence of 'first-time and/or unsophisticated investors', and economic slowdown revealing and aggravating the problems of the companies involved. Toms (2019) shows how clusters of technological changes enlarge the opportunities for fraud by increasing uncertainty and information asymmetry, with the asymmetry making it harder both for investors and regulators to monitor fraud (see also Hollow 2015), but whether this applies to all forms of fraud is open to question.

Disaster-related fraud

Fraud has also been found during and following natural disasters, such as floods, cyclones and bushfires, as well as industrial accidents (see Frailing & Harper 2017; Jackman 2017; Kerstein 2006), such as the BP Deepwater Horizon oil spill in 2010, following which 311 people had been convicted by September 2016, with 102 sent to prison, seven for five years or more (Crooks 2017). Following the Hurricane Katrina disaster in the United States in 2005, large numbers of false claims were made and over 1,300 prosecuted (Economist 2017).

Such was the level of fraud following Katrina that the US Department of Justice established the National Center for Disaster Fraud in the same year, and since then it has received over 100,000 complaints (US Department of Justice 2020). There have subsequently been large civil recoveries from contractors and public institutions making false claims. Risks generally relate to fraudulent charitable solicitations to support victims and their families, false insurance claims, consumer frauds involving repairs and recovery operations, and fraudulent applications for government relief and support payments (see Box 2). Historical examples have close parallels with the dishonest practices currently emerging during the coronavirus pandemic, although differing somewhat owing to the current reliance on digital technologies to commit fraud (see below).

Box 2: Fraud following the Grenfell Tower fire in London

In the early hours of Wednesday 14 June 2017 a fire broke out in the kitchen of Flat 16 Grenfell Tower, a high-rise residential building in North Kensington, West London. The fire claimed the lives of 71 people who were in the tower that night. An inquiry into the fire found that it was started by an electrical fault in a large fridge-freezer in the kitchen of Flat 16 but escaped into the cladding. Once established within the cladding, the fire spread rapidly up the outside of the building and firefighters were unable to fight it successfully. Within 20 minutes a vertical column of flame had reached the top of the building on the east side, from where it progressed around the rest of the structure, so that within a few hours it had engulfed almost the whole of the building (Grenfell Tower Inquiry 2019: 3).

Following the fire, the government offered residents emergency accommodation, a minimum £5,500 payment from the Grenfell Tower Residents' Discretionary Fund and new housing. In the months that followed, a number of individuals who claimed to have been sharing flats with residents who did not survive, fraudulently claimed emergency accommodation and other payments amounting to many hundreds of thousands of pounds.

By November 2019, Kensington and Chelsea council had paid out £775,000 to 16 fraudsters who have since been sentenced by the courts for claiming payments dishonestly. An additional eight cases are still being investigated or proceeding through the courts. As at November 2019, police had only recovered £24,000.

One of the most serious cases involved a 26-year-old man who claimed £81,000 in cash and free hotel stays as well as £11,000 towards a new permanent home, saying that he had lived in a Grenfell flat that actually had been occupied by a family of five who all died in the fire. He was charged with dishonestly making a false representation for accommodation and subsistence between June 2017 and June 2018 and sentenced to six years imprisonment (Daily Mail 2018).

Source: Daily Mail 2018; Gregory 2019; Grenfell Tower Inquiry 2019

Such disaster-driven frauds have also occurred in Australia. For example, on 31 July 1902, a serious mining disaster occurred at Mount Kembla in New South Wales. After a fortnight, on 16 August 1902, the *Sydney Mail* and *New South Wales Advertiser* (1902) reported that 'bogus collection frauds' were already circulating. The YMCA Sydney was falsely represented in an attempt to scam generous members of the public for donations 'to relieve the widows and orphans of the unfortunate men who lost their lives in so sudden and awful a manner' (Sydney Mail and New South Wales Advertiser 1902). Similar scams continued for over a year and spread across the country. On 11 December 1903, the *Geraldton Advertiser* (1903) in Western Australia published an article detailing a fake Art Union auto raffle whose proceeds were supposedly going to the widows and orphans of the deceased Mount Kembla miners but were never received. Similarly, during the Great Depression in the 1930s many street frauds occurred in Australian cities in which children were used to target the wealthy for donations (Morton & Lobez 2011).

Natural disasters in Australia, particularly bushfires and floods, also created opportunities for various types of fraud (see, for example, Canberra Times 1974). In 1939, private donors were targeted by individuals claiming to be from the Warrandyte Bushfire Relief Committee (Weekly Times 1939). One of the most extensive bushfire-related frauds followed the 16 February 1983 Ash Wednesday bushfires in South Australia. The then head of the Victorian-based National Safety Council of Australia used the aftermath of the bushfires to secure hundreds of millions of dollars in loans guaranteed with non-existent collateral. The funding was used for the safety council's expansion until the fraud was uncovered five years later (Morton & Lobez 2011). The Australian bushfires of 2019–20, which, in eastern Victoria alone, burnt 1.5m hectares of bushland, destroyed over 450 homes and forced 60,000 people to evacuate the area, also created many opportunities for dishonesty. The Victorian government response and recovery costs totalled $450m (Fowler 2020), a proportion of which was lost to fraud targeting both victims of the bushfires and those willing to donate funds, with over $400,000 recorded in losses to charity scams in 2019 alone (Cross 2020).

Flood relief fraud also used this approach, with one man jailed for falsely claiming funds on behalf of the Kempsey Flood Relief Committee (Newcastle Morning Herald and Miners' Advocate 1949). Another flood relief fraud occurred in Queensland, where a Brisbane woman falsely pretended to a Queensland Government flood relief official that her home had been damaged by floodwaters and received a relief payment.

Other disaster-related frauds have also occurred, including one in which insurers lost $50m in fabricated claims for repairs to homes damaged in the December 1989 Newcastle earthquake (Canberra Times 1991). Similar scams also quickly followed Cyclone Pam, which devastated the island nation of Vanuatu in March 2015, involving requests for donations from false Australian charities, the use of two fraudulent Instagram accounts, as well as people pretending to be from known Australian charities soliciting donations door-to-door and at shopping centres (Thomas 2015).

Fraud has also occurred following industrial and aviation accidents. On 10 February 1964, for example, the HMAS *Voyager* collided with the HMAS *Melbourne* off the coast of New South Wales and sunk, killing 82 military personnel. A fortnight later, a woman was arrested for pretending to be a relative of one of the deceased sailors in an attempt to gain financial benefits (Canberra Times 1964). The loss of Malaysia Airlines Flight MH17 over Ukraine on 17 July 2014, in which all onboard died, was quickly followed by the creation of a number of Facebook pages in the names of the 27 Australian victims seeking donations dishonestly (IFW Global 2014). Fraudulent spam emails using the names of confirmed victims were also sent out worldwide, promising large inheritances to beneficiaries willing to pay a settlement fee in advance (We Live Security 2014).

Technology as an enabler of fraud during pandemics

As the coronavirus pandemic developed in 2020, social distancing measures required people to remain in their homes, leading to intense reliance on digital technologies. 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. In one survey of 848 adults in the United States working from home due to COVID-19, 23 percent used personal devices for work, 37 percent re-used passwords for business purposes, and 53 percent indicated that their employer had no new security policies to manage personally identifiable information (Stupp & Rundle 2020). Two principal vectors have involved dissemination of consumer scams and the commission of payment system fraud.

Consumer scams during the COVID-19 pandemic

'As early as January 2020, cybersecurity companies like Kaspersky and Mimecast…reported several specific email phishing scams related to coronavirus' (Zirkle 2020: np). 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). The UK National Cyber Security Centre (NCSC) has noted phishing and malware related to health advice, contact tracing, funds and rebates, and fake goods and services—from PPE to disinfecting driveways (NCSC 2020). 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. The centre also worked with international allies to raise awareness of the threat to vaccine research. In July 2020, for example:

> …the NCSC revealed Russian cyber actors, known as APT29, had been targeting organisations involved in coronavirus vaccine development. The NCSC assessed that APT29, also named "The Dukes" or "Cozy Bear", almost certainly operated as part of Russian intelligence services. (NCSC 2020: 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:

> One of the new sites marketed an "oxygen concentration" machine for $3,080. Another had the "Corona Necklace Air Purifier", which for $59 claimed to provide "All Day Protection". A third offered a $299 pill that promised "Anti-Viral Protection" for 30 days. And sites such as CoronavirusGetHelp.com and test-for-covid19.com marketed home test kits for $29.99 to $79, none of which have been approved by the Food and Drug Administration (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 United Kingdom, for example, as early as 6 March, 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. On 9 March 2020, the US Food and Drug Administration and Federal Trade Commission issued joint warning letters to seven companies for selling fraudulent products claimed to prevent, treat, mitigate, diagnose or cure coronavirus disease (Zirkle 2020).

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. On 19 March, the UK Medicines and Healthcare products Regulatory Agency (2020) reported finding 2,000 online advertisements related to coronavirus and seizing over 34,000 fraudulent products, such as 'corona spray', 'coronavirus medicines' or 'coronaviruses packages'.

Since it was established in April 2020, the phishing reporting mechanism at the UK National Cyber Security Centre has helped them to take down over 300,000 malicious URLs linking to fake celebrity-endorsed investment schemes featuring famous faces such as Sir Richard Branson and Martin Lewis. Reports from the public to the NCSC's Suspicious Email Reporting Service, a pioneering system which received over 2.3m reports from the public between April and August 2020, resulted in more than 22,237 malicious URLs being blocked or taken down and 9,315 scams being taken down or removed, many relating to coronavirus scams. More than half of these URLs related to cryptocurrency investment scams (NCSC 2020). Whenever a change is announced, such as the requirement for over-75s to pay for BBC television licences, this leads to scam emails requesting personal financial information for harvesting. Between 1 September 2019 and 31 August 2020, the NCSC responded to more than 200 incidents relating to the United Kingdom's coronavirus response (28% of all incidents handled by the NCSC), with more than 15,000 coronavirus-related malicious campaigns taken down (NCSC 2020). In the previous three years since launching, the NCSC supported an average of 602 incidents annually—590 in 2017, 557 in 2018 and 658 in 2019 (NCSC 2020).

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). Financial losses in the United Kingdom have predominantly come from online shopping in which victims have ordered face masks, hand sanitiser and other PPE that fails to be delivered (Action Fraud 2020). There have also been reports of ticket refund fraud due to travel restrictions, romance fraud, charity fraud and financial loan fraud. 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, Malwarebytes Labs reported that 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.

Working from home due to social distancing requirements has created many opportunities for cyber-related fraud. Cybercriminals have exploited a legitimate US-based Microsoft support number for Australian customers. When Australians call the US 1800 support number, it redirects them to one registered by the scammers. Victims are asked to provide their name and date of birth for a call-back service. When the call is returned, the victim is instructed to download a remote access program giving the criminals direct access to their computer. The cybercriminal then convinces the user that their computer is compromised and due to COVID-19 measures they must pay a fee in untraceable cryptocurrency to correct the problem. The scammers have also attempted to gain access to bank account information and online banking apps during the remote access session (Australian Cyber Security Centre 2020).

The extent to which these are 'excess scams' (by analogy with 'excess deaths') is hard to identify, especially at this early stage. However, whether or not these scams would have happened anyway in a different format, these examples 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 January and November 2020, 4,850 COVID-19 related consumer scams worth $5.8m were reported to the ACCC's Scamwatch reporting portal (www.scamwatch.gov.au). Although representing only 3.3 percent of all scams reported to Scamwatch during this period, the reports that mentioned COVID-19 commenced almost immediately following the onset of the pandemic in early 2020 (ACCC 2020). Data provided by the ACCC (2020) show the substantial increases in COVID-19 related scams reported during 2020, in terms of both numbers and dollar losses (Figure 6).

Figure 6: Cumulative number and value of COVID-19 scams reported to Scamwatch, March to November 2020

Note: Number and value of reports made to Scamwatch in the calendar years preceding the weeks ending March to November 2020 in Australian dollars

Source: Data derived from ACCC 2020

Technology has also facilitated the sale of medical supplies and PPE during the coronavirus pandemic in 2020. 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, Ball & Jiang 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. Three markets accounted for 85 percent of all unique listings identified. Of the 110 vendors identified, eight were active in multiple markets. A small proportion of vendors accounted for most listings and the estimated value of all unique listings was A$369,000. PPE accounted for nearly half of all unique listings, and one-third of products were antiviral or repurposed medicines.

Supposed vaccines, tests and diagnostic instruments each accounted for nearly 10 percent of listings. Apart from fraud, details about the origin or composition of vaccines were sparse. These products may have been diverted from animal or human trials, or even sourced from recovered COVID-19 patients. The median cost of a vaccine was A$575, but vaccines offered by three vendors on DarkBay allegedly sourced from China were priced at US$10,000 to US$15,000. The most costly vaccine was 'COVID-19 Antidote for sale' at A$24,598 on Dream Alt, shipped worldwide from the United States (Broadhurst, Ball & Jiang 2020). As the global rollout of genuine COVID-19 vaccines continues during 2021, it is likely that various acts of dishonesty will occur, including theft of intellectual property, product substitution, and procurement and invoicing fraud on governments.

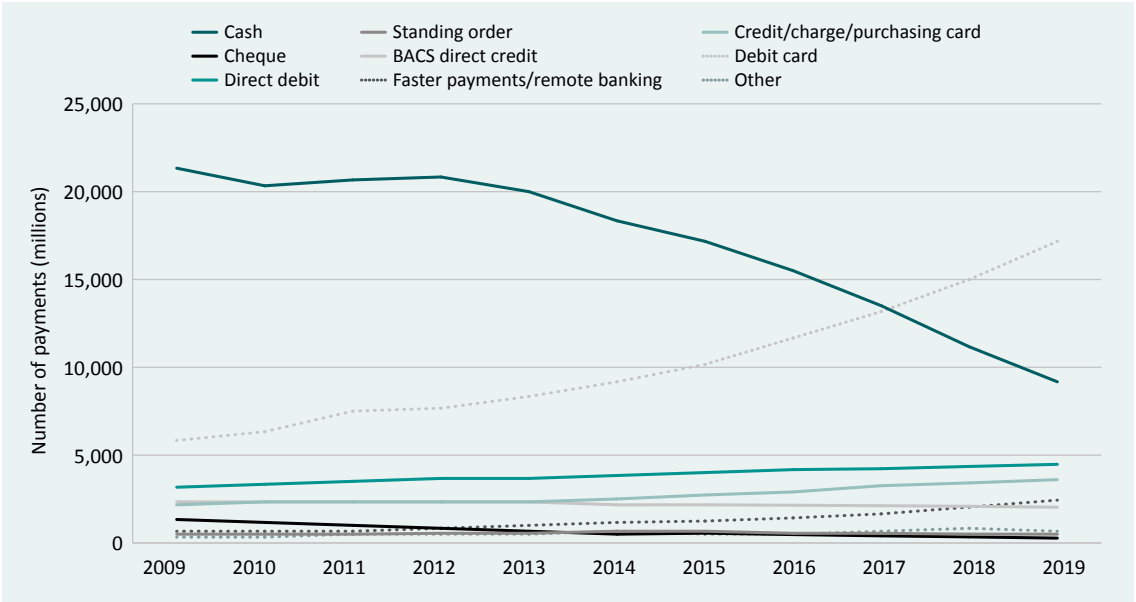
Some scams are not directly related to COVID-19 but are aggravated by remote working risks. In the United Kingdom and elsewhere, employees have received emails purporting and appearing to be from their managing directors. The message asks the recipient to carry out a task and requests their phone number. The recipient then receives a WhatsApp message with a convincing profile picture asking them to go to the supermarket to purchase one or more Google Play cards and provide the numbers for the cards. Before COVID-19, such requests might have been more likely to be questioned. The NCSC (2020) have also warned about an Office 365 phishing email. Fraudsters send employees an email pretending to be from their organisation's IT department. It requests that users update the VPN configuration used to access the company network while working from home. Users who click the link in the email are directed to a fake page that looks identical to a legitimate Office 365 login page.

Payment card fraud and economic crises

While corporate insider and investment frauds and interpersonal scams of different kinds have been present for centuries, and certainly throughout the 102-year period of this review, particular forms of fraud have become possible only through the development of particular technologies, such as payment cards. Before 1974, only store-issued cards were used in Australia, with Diners Club and American Express credit cards accessible to the wealthy. In 1974, the Bankcard was launched by Australian banks who had developed their own card network and implemented the technology needed for a nationwide shared facility. By 1976, there were 1,054,000 Bankcard holders and almost 49,000 participating merchants. The first ATMs began popping up in Australia in 1977, and by 1978 Bankcards could be used across the nation for cash withdrawals and purchases (see Smith 1998).

A similar sequence of events occurred in the United Kingdom, with the first credit card being issued in 1966 (with limited international interoperability) and the first debit card in 1987. The United Kingdom now has one of the most mature payment card markets in the world. Figure 7 sets out payment types 2009–2019 (European Central Bank 2020; UK Finance 2020b), within which payment fraud opportunities take place. In the first half of 2020, losses due to unauthorised financial fraud using payment cards, remote banking and cheques decreased eight percent, to £374.3m (UK Finance 2020b).

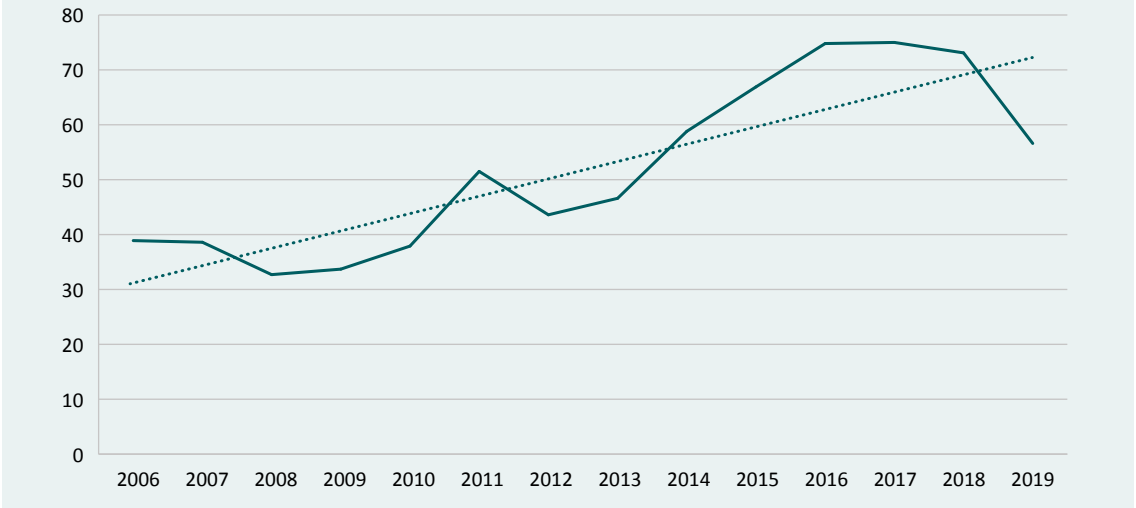
Figure 7: Payment types used in the United Kingdom, 2009–19



Source: Data derived from European Central Bank 2020 and UK Finance 2020b

In Australia, national payment card fraud statistics are published by the Australian Payments Network (AusPayNet, formerly known as the Australian Payments Clearing Association; APCA (2014) and AusPayNet (2020a)). In the decade surrounding the global financial crisis, payment card fraud showed an initial decline followed by an increase once the crisis was largely over. Figure 8 shows the rate of fraud on debit, credit and charge cards (as operated by American Express, Diners Club International, eftpos Payments Australia, Mastercard and Visa) in terms of value (cents per $1,000 in transactions) perpetrated in Australia and overseas on Australian issued cards between 2006 and 2019. The sharp decline in payment card fraud was due to the introduction of the Card-Not-Present Fraud Mitigation Framework in July 2019, a whole-of-industry approach to fraud prevention (AusPayNet 2020a).

Figure 8: Rate of fraud on scheme debit, credit and charge cards perpetrated in Australia and overseas on Australian issued cards, 2006–19 (cents per $1,000 transactions)



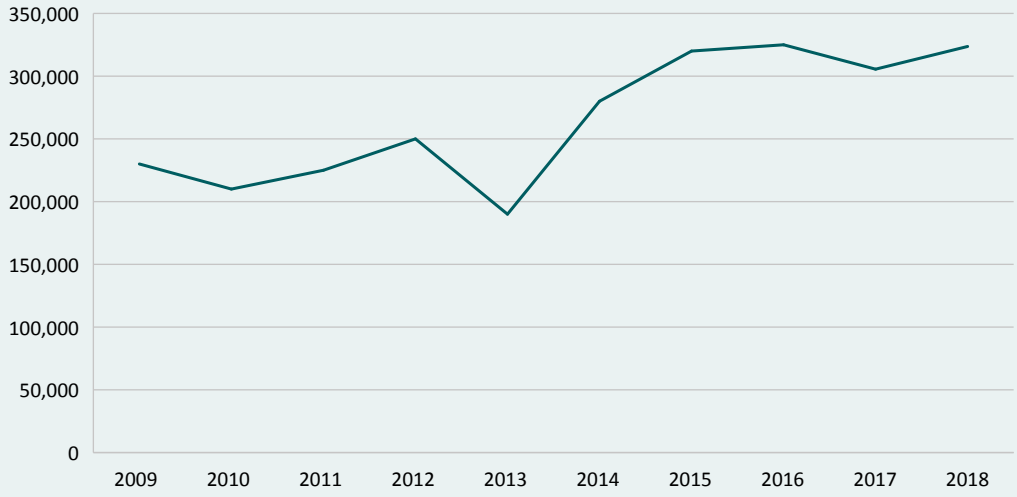
Source: AusPayNet 2020a; Australian Payments Clearing Association 2014

Here are the trends since the last economic crisis (see Levi & Smith 2011). In the United Kingdom, data collected by the not-for-profit fraud prevention service Cifas (2009a, 2009b) indicated a rise in identity takeover frauds, as 'new credit' became harder to get, generating displacement to impersonating existing account holders. Such frauds emerge quite quickly. At the end of the third quarter of 2009, Cifas data showed an 11 percent increase in the level of fraudulent activity, and a 38 percent upturn in misuse of facility fraud (where an account, policy or other facility is used fraudulently) when compared with the same period in 2008. By 2010, a decrease in the number of frauds was evident across most fraud types (Cifas 2011).

The most notable was the 23 percent decrease in the number of application frauds on new accounts, reflecting both restricted lending by organisations affecting new applications (both genuine and fraudulent) and the more stringent lending criteria used by organisations when making lending decisions. Cifas (2009b) data reveal that over 59,000 victims of impersonation were recorded in the first nine months of 2009—a 36 percent increase from the same period in 2008. The overall number of identity frauds increased by a third in the first nine months of 2009 from 2008, with account takeovers rising by 23 percent in 2009 compared with the same period in 2008, and by 238 percent in the last 24 months. More than one in two account takeovers have targeted victims' plastic card (ie credit card) accounts, and mobile phone account takeovers more than doubled in 2009 from 2008 levels. The one-third rise in identity fraud (using other people's identities) between 2008 and 2009 flattened out in 2010, possibly because the industry reacted to the identity fraud boom with better monitoring.

Cifas monitoring shows that the rate of credit fraud recorded by the financial sector was as indicated in Figure 9.

Figure 9: Industry-identified credit fraud cases in the United Kingdom, 2009–2018 (*n*)



Source: Cifas 2019

The highest number of cases ever recorded on the National Fraud Database occurred in 2019—364,643 cases, up 13 percent on 2018. Identity fraud made up 61 percent of total cases, nearly a quarter of which involved misuse of facility. A substantial increase in facility takeover and cases involving insiders also occurred in 2019 (Cifas 2020). So identity fraud cases rose from 77,642 cases in 2008 to 223,163 in 2019. The amount of money involved is not available, but Table 1 (below) shows no corresponding rise in losses from payment card identity theft over this period.

In Australia, trends in identity crime and misuse have been tracked by the Australian Institute of Criminology since 2014, with the report for 2018–19 finding direct and indirect costs of $3.1b, a 17 percent increase on costs in 2015–16. The top three types of personal information most often reported as having been misused in Australia between 2017 and 2019 were names, credit/debit card information and bank account information (Franks & Smith 2020). These three types of personal information have continued to have the highest ranking since 2013 (Smith & Hutchings 2014).

Between 2006 and 2009, UK payment card fraud data displayed a number of trends:

- a broad downwards trend in fraud on lost or stolen cards due to the introduction of chip-and-PIN in Europe;
- a later (2009) drop in counterfeit frauds on skimmed and cloned cards, which previously had risen substantially, mainly through being used overseas to sidestep chip-and-PIN controls;
- a slower, modest rise in cards obtained by identity theft; and
- a less easily explained drop in card-not-present frauds over the phone and internet (UK Payments 2009).

In concert with the fall in cheque usage, cheque fraud losses fell significantly, while online banking fraud losses rose 55 percent to £39m in the first half of 2009—perhaps due to improved awareness and reporting, but also reflecting increased phishing for passwords and sophisticated cloning of bank websites.

The most recent data on financial fraud in the United Kingdom, for January to July 2020, have shown losses due to unauthorised transactions on cards, cheques and remote banking declining to £374.3m, down by eight percent on the previous year. The number of recorded cases of unauthorised fraudulent transactions rose by one percent to 1.4m. UK Finance (2020a: 6) reported:

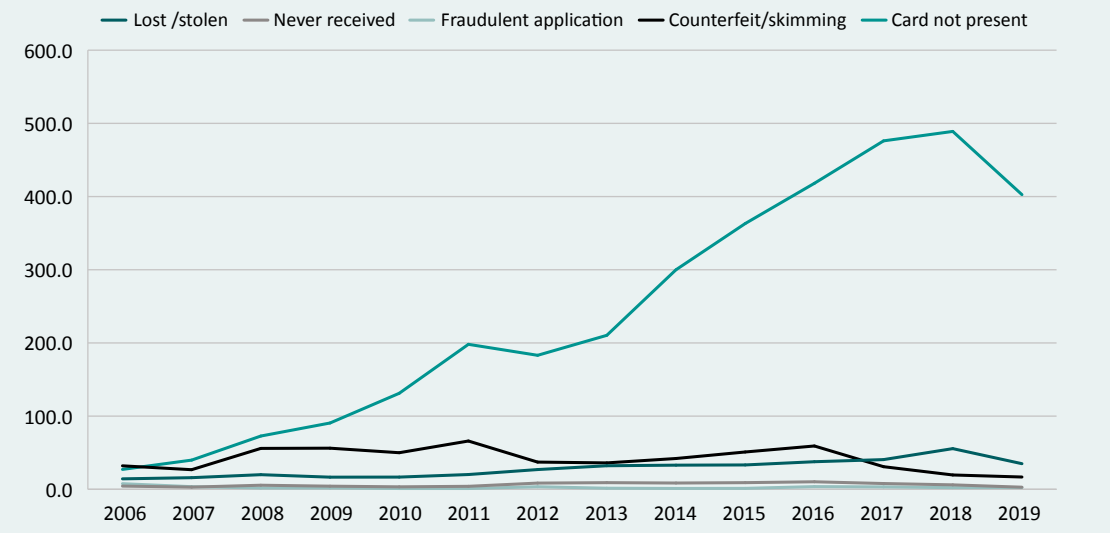
> “Total losses due to authorised push payment [APP] scams were £207.8 million in the first half of 2020, static compared to the same period in 2019. The number of cases rose 15 percent to 66,247. Purchase scams form the highest volume of APP scams and rose by six percent to 37,516, but it was impersonation scams – police/bank scam cases – which saw the biggest increase, rising 94 per cent to 8,222.

In the first half of 2020, during the pandemic, 'social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, was a key driver of both unauthorised and authorised fraud losses' (UK Finance 2020a: 6) with much of this arising from opportunities for deception created by the pandemic. For example:

> Criminals may…get in touch claiming to be from an airline or travel agency, offering refunds for flights or holidays that have been cancelled due to the pandemic. Additionally, criminals are exploiting the growing numbers of people working remotely, by posing as IT departments or software providers and claiming that payments are needed to fix problems with people's internet connection or broadband. There is sometimes a delay between criminals obtaining people's details through these scams and using them to commit fraud. (UK Finance 2020a: 7–8)

In Australia, overall losses on all Australian card types for different crime types are shown in Figure 10.

Figure 10: Value of frauds for all Australian payment card types by crime type, 2006–19 ($m)

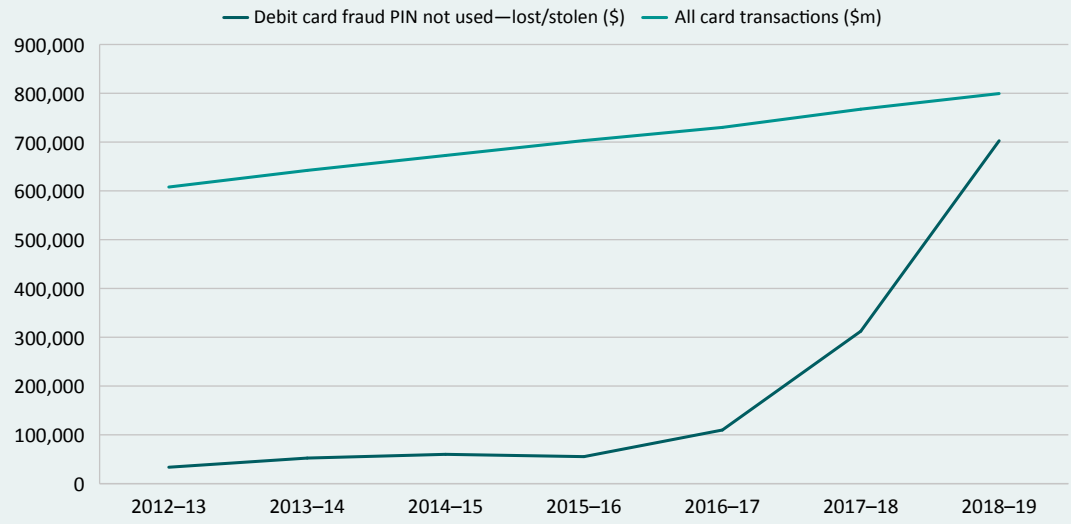


Source: AusPayNet 2020a; Australian Payments Clearing Association 2014

The value of card-not-present fraud increased considerably, apart from declines in 2012 and 2019, although as a proportion of the value of all card transactions it has declined since 2015. Card-not-present fraud still remains the most prevalent type of fraud on Australian cards but declined sharply in 2019 with the introduction of new industry fraud control measures (AusPayNet 2020a). The value of fraud involving lost and stolen cards has shown a gradual increase since 2006 with no observable change around the time of the global financial crisis, but also declined between 2018 and 2019.

Since 2015–16, however, the value of fraud involving lost and stolen debit cards in which PINs were not used increased at a much higher rate than the value of all debit card transactions, perhaps due to the increased reliance on contactless debit card transactions over this period (Figure 10). This trend is likely to continue during the coronavirus pandemic, as a continuation of the trend below (Figure 11).

Figure 11: Value of debit card frauds involving lost and stolen cards in which PINs were not used, 2012–19 ($)



Source: AusPayNet 2019

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).

Table 1: UK issued payment card fraud losses, United Kingdom 2010–19 (£m)

Fraud type	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	% change 2010–19
Remote (CNP)	226.9	221	247.3	301	331.5	398.4	432.3	408.4	506.4	470.2	+207
e-commerce[a]	(135.1)	(139.6)	(140.2)	(190.1)	(219.1)	(261.5)	(310.3)	(310.4)	(394.2)	(359.3)	(+266)
Counterfeit	47.6	36.1	42.3	43.3	47.8	45.7	36.9	24.2	16.3	12.8	–269
Lost & stolen	44.2	50.1	55.4	58.9	59.7	74.1	96.3	92.9	95.1	94.8	+224
Card ID theft	38.1	22.5	32.6	36.7	30.0	38.2	40.0	29.8	47.3	37.7	–1
Card non-receipt	8.4	11.3	12.8	10.4	10.1	11.7	12.5	10.2	6.3	5.2	–38
Total	**365.2**	**341**	**390.4**	**450.2**	**479.1**	**568.1**	**618.1**	**565.4**	**671.4**	**620.6**	**+170**
UK	271.4	260.9	288.4	328.2	328.7	379.7	417.9	407.5	496.6	449.9	+166
Fraud abroad	93.9	80.0	102.0	122.0	150.3	188.4	200.1	158.0	174.8	170.7	+182

a: Figures in parentheses are the e-commerce losses forming part of CNP totals
Note: CNP=card-not-present. These figures cover fraud on debit, credit, charge and ATM only cards issued in the UK
Source: UK Finance 2020b

In the United Kingdom, card fraud losses as a proportion of the amount spent on UK-issued cards decreased during 2019, falling from 8.4p per £100 spent in 2018 to 7.5p per £100 in 2019. In 2008 it was 12.4p for every £100 spent (UK Finance 2020b), but in the first half of 2020, the rate again rose to 8.4p per £100 spent (UK Finance 2020a). The fraud to turnover ratio is almost the same at 0.075 as it was in 2010 (0.074), though with fluctuations up and down in between. While losses have been decreasing, the number of confirmed cases (ie accounts defrauded, not individuals) increased during the same period, rising by five percent to 2,745,539 cases in 2019. This reflects quicker detection and stopping of accounts by card issuers, with a lower average loss per account defrauded (£381 in 2010, down to £226 in 2019, and £210 in the first six months of 2020; UK Finance 2020a).

Comparing the United Kingdom with Australia in 2019, card fraud as a percentage of all card spending was 0.075 percent in the United Kingdom and 0.057 percent in Australia. Card fraud was 75 percent of all payment fraud in the United Kingdom and 92 percent in Australia, and card-not-present fraud was 76 percent of all card fraud in the United Kingdom and 87 percent in Australia (AusPayNet 2020a). 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.

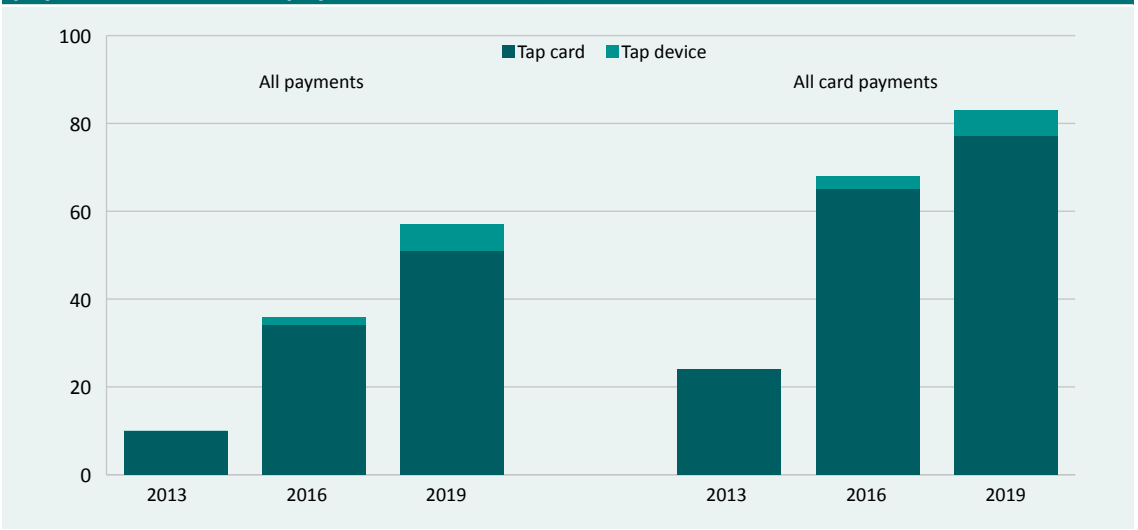
Cash use and pandemics

In most developed countries, cash is being used much less often than in the past. In Australia, for example, cash accounted for only 27 percent of consumer payments made in 2019, down from 69 percent in 2007 (Caddy et al. 2020). At present, the vast majority of payments are now made using cards (9,452m payments on Australian-issued cards worth $767b in 2017–18, increasing from 5,871m payments worth $608b in 2012–13). In 2018–19, the number of ATM withdrawals in Australia dropped to 577m, 20 percent fewer than in 2014–15 (AusPayNet 2020b).

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. In some countries, banknotes were collected and quarantined due to concern that they might be contaminated with the virus (King & Shen 2020). In the United States, the Federal Reserve began quarantining cash repatriated from Asia before sending it back into circulation because of contamination risks, while the National Reserve Bank of South Africa released a public warning that people purporting to be bank representatives had been 'collecting' banknotes believed to be 'contaminated' with coronavirus (Cash Essentials 2020).

To minimise these risks, the use of contactless payment cards has been promoted. In Australia, for example, on 8 April 2020, the contactless card payment PIN limit increased from $100 to $200 to encourage use of contactless payments (AusPayNet 2020b), and some merchants accepted only contactless card payments for all transactions. Examples include petrol outlets, local council offices and utilities. Since 2013, the number of both card payments and all payments using contactless tap technologies has increased substantially in Australia (Figure 12).

Figure 12: Point of sale contactless card payments in Australia as a proportion of all payments and all card payments, 2013–19 (%)



Source: Caddy et al. 2020: 12, based on Reserve Bank of Australia calculations using data from Colmar Brunton, Ipsos and Roy Morgan Research

However, many consumers continue to use cash for a variety of reasons. The Reserve Bank of Australia's Consumer Payments Survey in 2019 found that Australians prefer to use cash because of merchant acceptance (32%), convenience for small transactions (21%), to aid budgeting (15%) and to protect privacy and prevent fraud (8%; Caddy et al. 2020).

Similar trends away from cash and towards tap payments exist in the United Kingdom and in Europe as a whole (Thomas & Megaw 2020). In early 2020, ATM transactions during COVID-19 restrictions were less than half of those of the same period the previous year. Fewer than 10 percent of those aged over 45 were registered for mobile payments in 2019, but this, alongside internet use, has increased among older age groups in 2020. Contactless payments accounted for 21 percent of all transactions in 2019 (up from 3 percent in 2015), and these have accelerated with the raising of the maximum tap payment from £30 to £45 from 1 April 2020. Contactless fraud on payment cards and devices remains low, with £20.6m of fraud losses during 2019 compared to spending of £80.5b over the same period. This is equivalent to just 2.5p in every £100 spent using contactless technology. Contactless fraud on payment cards and devices represents 3.3 percent of overall card fraud losses, while 44 percent of all card transactions were contactless in 2019. Data on fraud losses during 2020 are not yet available, but Mastercard report that during the COVID-19 pandemic, 66 percent of their transactions (by volume) were contactless. The financial risks per card from the increased limits for contactless payments are managed by occasionally requiring cardholders to input PINs.

Cash is not only used for legitimate financial transactions but also an important facilitator of economic crimes such as money laundering, counterfeiting, welfare and tax fraud and other organised criminal activities, most notably drugs and vice (Europol 2006, 2017). Although physical currency has long been thought to be the chosen payment channel used by criminals owing to its anonymity and inability to be traced, especially in pre-cryptocurrency times (Bell 2004), information is lacking on the extent to which criminals use cash and how this has changed over time. Trends in criminal intelligence are likely to show an increased overall use of cash during the pandemic to facilitate economic crime, particularly relating to government stimulus eligibility requirements. Hoarding cash, for example, is one way to circumvent eligibility requirements for economic stimulus and support payments. Results of the Consumer Payments Survey (Caddy et al. 2020) found that cash hoarding accounts for between 10 and 20 percent of total banknotes in circulation in Australia; however, the Reserve Bank of Australia believes this number to be misleading, as those who hoard cash are less likely to participate in such surveys (Finlay, Staib & Wakefield 2018). The Currency (Restrictions on the Use of Cash) Bill 2019 (Cth), which is currently before the Australian Parliament, was introduced to counteract this type of activity.

Fraud arising from COVID-19

In November 2019, a new strain of coronavirus (SARS-CoV-2) was identified in Wuhan, Hubei Province, China. Since then, this new coronavirus has taken on pandemic status and by 19 December 2020 affected 215 countries, with 74m confirmed cases and 1.7m deaths (WHO 2020). In Australia between 22 January and 19 December 2020, there were 28,128 confirmed cases and 908 deaths (Department of Health 2020).

During the COVID-19 pandemic, Australia managed to suppress community transmission of the virus quite well initially until a number of outbreaks occurred. One of the early outbreaks took place in New South Wales in March 2020 when a cruise ship, the *Ruby Princess*, docked in Sydney harbour and allowed its passengers to disembark without adequate virus screening or quarantine. A number of passengers and crew were infected and as they entered the community the virus spread rapidly. This led the NSW Government to appoint a Special Commission of Inquiry to investigate the circumstances surrounding the matter, which reported on 14 August 2020 (Special Commission of Inquiry into the Ruby Princess 2020).

Then in Victoria in May 2020, COVID-19 spread from a number of quarantine hotels to the community in Melbourne and nearby suburbs. A Board of Inquiry in Victoria was commissioned to examine this, with a final report filed on 21 December 2020 (COVID-19 Hotel Quarantine Inquiry 2020).

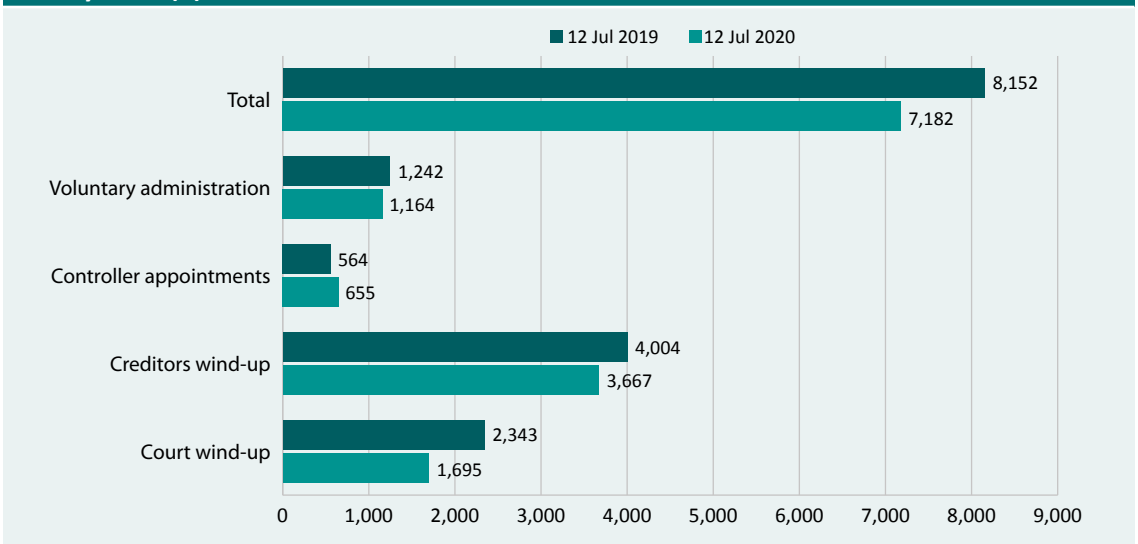
Government responses to these and other outbreaks led to isolation of some sections of cities, the imposition of stay-at-home lockdown orders, curfews, mandatory wearing of face masks and closure of state borders. Travel bans have also been imposed on both international and some internal flights in Australia, and gatherings in public banned with schools and other institutions closing for face-to-face activities and with business being conducted online. The effect on the economy was considerable, with an expected Australian Government budget surplus of $6.1b for 2020–21 being replaced by an underlying cash deficit of $214b for 2020–21, or 11 percent of GDP (Australian Government 2020).

Quantifying the problem

The recession in Australia created all the elements needed for economic crime to occur or be discovered. As noted above, quantification of the problem is hampered by a number of factors. First is the problem of determining the causal relationship between the pandemic and frauds that are detected. As in previous pandemics and economic crises, 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 and the influence of the pandemic is only indirect in allowing them to be identified. This is particularly the case with long-firm fraud and frauds that have continued undetected for many years, as often occurs with high-value economic crimes within organisations (Association of Certified Fraud Examiners 2020).

Evidence for this comes from the number of companies in Australia that have entered external administration. Figure 13 shows that in the 12 months to 12 July 2020, the numbers decreased by 12 percent on a 12-month rolling average (apart from controller appointments, which increased slightly). This indicates that many companies that normally would have failed are being artificially supported by government payments. Similar patterns exist in the United Kingdom, for similar reasons, and we can expect large rises in businesses entering administration following the diminution or ending of such payments. Although not necessarily indicative of fraud, there is the possibility that 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). Concern has been expressed in the United Kingdom about the potential abuse of pre-pack administration to enable directors to repurchase the assets from their businesses cheaply and walk away from their corporate debts.

Figure 13: Australian companies entering external administration, 12 July 2019 to 12 July 2020 (*n*)



Source: Australian Securities and Investments Commission 2020 (Chart 1B.3)

The second difficulty in quantifying fraud arising from pandemics and economic shocks 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 victimisation surveys. Interestingly, as noted above, 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 2020).

For example, the ATO 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). Equivalent numbers of extra staff are unavailable in the United Kingdom (or the United States), but the National Cyber Security Centre, the City of London Police, the National Economic Crime Centre, UK Finance and the Cabinet Office Counter-Fraud teams as well as the Fraud Advisory Panel have been actively involved in monitoring and advising consumers and others how to avoid COVID-19 fraud victimisation in the United Kingdom. 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).

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). HMRC's fraud hotline had received over 10,000 reports by November 2020 and 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. 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.

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 United Kingdom, 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 has led to a substantial increase in government-funded support payments being made. The *Coronavirus Economic Response Package Omnibus Act 2020* (Cth), which contains 16 schedules of support measures, was developed to address the significant economic consequences for businesses and individuals arising from the COVID-19 pandemic (Treasury 2020a). Such measures include the JobKeeper program, which allows businesses to retain staff and pay them a base salary if they meet certain criteria; the JobSeeker program, which provides increased payments to individuals looking for employment; and various tax relief measures for small and medium businesses designed to ease the economic burden created by the pandemic. Because of the substantial value of these programs, some individuals and corporations have sought to defraud the government in a variety of ways. 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 (Box 3). In other cases, businesses have registered for JobKeeper payments but illegally withheld a proportion of the funds from their employees (Palmer-Derrien 2020). Although not dishonest, many individuals have also received salary supplements from the government in amounts that exceeded the salaries they had been receiving prior to the pandemic. These payments have been justified as a consequence of the speed with which support payments were made and the fact that any additional payments would, nonetheless, assist the Australian economy generally. 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.

Box 3: Case studies of economic stimulus payment fraud in Australia

Two women in Port Macquarie, New South Wales were charged with fraudulently obtaining more than $27,000 in COVID-19 JobSeeker and bushfire recovery assistance payments. The two women had already obtained $10,000 and had made claims for a further $17,000. The alleged frauds were uncovered when Services Australia (formerly the Department of Human Services) identified a pattern of suspicious activity and referred the matter to the Australian Federal Police. The allegations included 25 fraudulent claims for the Australian Government Disaster Recovery Payment made following the 2019–20 bushfires. Each woman was charged with eight counts of obtaining a financial advantage by deception.

In another case, Australian Federal Police arrested a Western Sydney man who allegedly assumed 53 fictitious identities in order to make 65 fraudulent claims for bushfire recovery payments and JobSeeker payments. They charged him with several offences including obtaining a financial advantage by deception.

Source: Services Australia 2020; Sutton 2020

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. A proportion of this was provided to individuals who had dishonestly made claims outside the strict eligibility requirements, or to individuals who sought to steal funds by making unauthorised applications for early release payments from other members' accounts without their knowledge or permission (Box 4). 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).

Box 4: Case study of alleged fraud involving early access to superannuation funds

In late May 2020, a Perth woman was charged with allegedly submitting multiple false claims to gain early access to superannuation (Sutton 2020). Police alleged that the woman submitted several false hardship claims on behalf of other people to access superannuation payments of $10,000 each. The case was detected by the joint Australian Federal Police and Department of Human Services (now Services Australia) Taskforce Iris, which was formed in July 2019 to investigate serious welfare non-compliance and criminal activity in connection with bushfire benefit payments (Services Australia 2019). Taskforce Iris investigators 'seized several documents, $1,750 cash, ink-based business identification and certification stamps, and electronic devices' as part of the investigation (Hickey 2020: np).

In August 2020, the Australian Federal Police charged three Queensland women with allegedly trying to defraud the Australian government's early access to superannuation scheme of more than $113,000 by submitting false claims to gain access to other people's superannuation holdings (Swanston 2020).

Sources: Hickey 2020; Services Australia 2019; Sutton 2020; Swanston 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. The Job Retention (Furlough) Scheme was introduced to protect jobs and to help employers and families through the pandemic, with the government agreeing to pay up to 80 percent of people's wages to a maximum of £2,500 a month. The scheme was extended to the end of April 2021 and by December 2020 provided approximately £20b in respect of 10m jobs. Workers covered by the scheme were not, however, permitted to work for their employer while on the scheme (Tew 2020; Welford 2020). 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). This is, however, based largely on anecdotal evidence to date, and 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, 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 16 August 2020, the Coronavirus Business Interruption Loan Scheme approved £13.6b in expenditure; the Coronavirus Large Business Interruption Loan Scheme approved £3.5b; and the Bounce Back Loan Scheme, £35.47b (HM Treasury 2020).

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 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. Although not yet quantified, the scale of fraud and error involved in these programs, in both Australia and the United Kingdom, is costly. The expenditure could, however, be justified on the basis that stimulus had to be provided immediately, and that the funds provided would nonetheless assist the national economic recovery despite being provided outside the eligibility rules. Most of the media and political pressures to date have been on the non-provision or delayed provision of aid to needy businesses and individuals rather than on fraud risk reduction, though it is reasonable to anticipate that individual cases of abuse and alleged procurement corruption will receive significant attention when published, as will any audit reports.

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, it is reasonable to conclude that 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 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 report has not specifically analysed, first-hand, the motivations of fraud offenders, although it is clear from the above that coronavirus fraudsters are motivated by a mixture of economic need, created by a decline in business activity and loss of jobs, and personal greed driven by apparent opportunities to gain access to government support payments during a time of a perceived reduction in fraud controls. 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 & Free 2020; Schuchter & Levi 2015). The 2020 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:

- denial of authorship—'I'm acting on behalf of others, perhaps under duress or coercion';
- sharing responsibility—'Everyone's doing it—the government can afford it and the funds taken will be spent, thus supporting the economy';
- external influences—actions are caused or necessitated by the pandemic, thus reducing personal responsibility;
- denial of injury—the conduct was designed to keep an organisation afloat and the funds will be repaid when the economy improves;
- denial of illegality—where eligibility for stimulus measures is unclear, the conduct may be seen as not technically illegal;
- denial of culpability—dissatisfaction with current or expected future employment situation or reasons for job loss may be seen to reduce culpability, especially where the unpunished misconduct of senior personnel can be pointed to as a negative role model; and
- appeal to higher loyalties—laws can be ignored due to higher duties owed to family and friends during the pandemic.

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 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 & 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.

Such rationalisations, Andon and Free (2020) argue, apply most often to 'a static phenomenon involved in the initial decision to offend' rather than to continuing patterns of dishonesty. Using data from interviews with individuals convicted of serious fraud offences in Australia, Andon and Free (2020) identified a number of strategies that were used to cope psychologically with the strain of ongoing fraudulent conduct: problem-focused, emotion-focused and social-focused coping strategies. As the pandemic continues—perhaps for years, continuously or intermittently—such coping strategies are likely to become apparent, once the immediate need to act illegally dissipates. Although the rationalisations noted above may have been present during the initial decision to commit fraud at the beginning of the pandemic, it is likely that coping strategies will take their place to remove or lessen the strain and psychological stress caused by ongoing fraudulent behaviour.

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 & Levi 2020; HM Inspectorate of Constabulary and Fire & Rescue Services 2019; Levi & 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, 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 corporations and consultancies 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 persistent efforts at business email compromise, data breaches, and ransomware have abounded in recent years, and prevention efforts need to be disciplined at all times to be effective. 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 (Cavaglieri 2020; UK Finance 2020b). 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).

Conclusions for Australia: Near future fraud and fraud control trends

What has been learnt from the past

This report has reviewed the drivers and consequences of a number of pandemics and financial crises that have occurred since the First World War, commencing with the Spanish flu in 1918–19 and ending with the COVID-19 pandemic of 2020. On each occasion, the crisis was preceded by indicators that usually went unheeded or the response was delayed until the scale of the problem became obvious and containment invariably difficult to achieve. Although response measures of varying degrees of utility were adopted during and following each crisis, formal evaluation of these measures was rarely undertaken. This led to less than satisfactory preventive strategies being developed and adopted to deal with similar events in the future. Of course, it could be argued that problems arising from natural disasters and pandemics on this scale can never be prevented. However, some of the consequences of these events recur following each event and if knowledge of the past had been used effectively, some of the harms could have been avoided. Preventing some if not all fraud is an obvious case in point.

One recurring theme is the focus of the present study—the tendency of individuals and organisations to act dishonestly to compromise controls on government-funded recovery and support programs for immediate gain. Although empirical evidence is limited, anecdotal accounts are available to document the presence of fraud during and following each of these global events that not only prevented fair distribution of limited resources to the affected communities, but also exacerbated the economic harm to communities globally.

The Australian economy has been affected to varying degrees by each of the pandemics and economic crises described above, and, like other nation states, Australia has learnt the lessons of the past only to a limited extent. The fact that Australia has suffered lower levels of health and economic consequences from each of the global crises than other developed Western nations has been due more to its geographical isolation, general financial stability, relatively small population and stable government than to any other factors. Despite these protective factors, the economic recovery following each crisis took at least a decade to occur. Some of the consequences of these crises for Australia are described below.

Spanish flu 1918–19

As in the COVID-19 pandemic in 2020, risks of infection from the Spanish flu arose in Australia initially from maritime arrivals that were, at that time, the only way in which individuals could enter the country. Responses from each of the states and territories were, in 1919, poorly coordinated, leading to quarantine regimes differing across jurisdictions. Governments subsequently identified this as a concern, by governments leading to the establishment of the Commonwealth Department of Health in 1921.

In 2020, 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.

Second World War, 1939–1945

In Australia during the Second World War, rates of fraud declined because large numbers of men took on war service, which made them unavailable to exploit local opportunities to commit fraud. On their return to civilian life following the war, rates of reported fraud rose as the economic consequences of wartime were felt by the workforce and as opportunities arose when the economy began to improve.

One area of economic crime that was enabled by wartime related to profiteering and price gouging in connection with food, medicines and commodities in the Australian community. Although this resulted in some prosecutions, regulation was generally inadequate. In 2020, during the COVID-19 pandemic, profiteering once again occurred during lockdowns, for products in high demand—face masks, hand sanitiser, toilet paper—as those in affected communities feared loss of supplies and an anticipated inability to obtain necessary goods when confined to homes and suburbs, despite having access to online shopping. Once again, the lessons learnt about postwar restrictions had been forgotten, or were unknown to Australians 75 years later.

Global financial crisis, 2008–09

The Australian Government acted quickly during and after the global financial crisis in 2008–09 to create a range of stimulus measures including a school building program, home insulation scheme and a solar, green energy and water renovation plan. These were, arguably, implemented too quickly, leading to wasted resources and some unsafe practices implemented. The economic stimulus, however, prevented the Australian economy from deteriorating as much as in other countries, with unemployment reaching only five percent following the crisis, the average for the whole twentieth century.

In 2020, the Australian Government's stimulus packages were introduced more slowly than those following the 2008–09 crisis, but wastage was still present despite efforts being taken to deter and prevent fraud from occurring. However, the economic harm of the pandemic in 2020 was far greater than that of any other crisis that affected Australia, although it remains to be seen exactly how much coronavirus-related fraud cost the economy. By mid-2020, the unemployment rate in Australia was 7.5 percent, similar to the rate shortly after the turn of the twentieth century and also during the Asian financial crisis in the early 1990s (11%), but less than the 20 percent seen during the Great Depression (ABS 2020).

Australian bushfires, 2019–20

In Australia, natural disasters, especially bushfires, have occurred regularly and with increasing severity due to the changing climate. The most recent bushfires in late 2019 and early 2020, occurred just prior to the onset of the COVID-19 pandemic, making it difficult to disaggregate the effects of these two crises. Governments provided immediate and extensive support to those who had lost loved ones, homes and businesses during the bushfires (Fowler 2020), and difficulties were experienced in identifying victims whose personal identification records had been destroyed. This provided opportunities for fraud, as well as a range of insurance, charity and consumer scams associated with relief packages (Cross 2020).

During the COVID-19 pandemic, identity misuse once again occurred, with a number of fraudulent claims for support payments being made using false or fabricated identity credentials. Technological solutions to control fraud were heavily relied on in both the bushfires and the coronavirus pandemic but found to be wanting due to community concerns regarding security of personal information and some technological problems.

The cost of pandemics

As we have seen from this brief review of some of the global economic shocks and pandemics since the Spanish flu, there is little information available on the cost of fraud and economic crime arising from these events. Some data are available on the economic impact and effects on employment and the extent of government deficits, but quantification of the cost of fraud and dishonesty associated with these events remains scant. The COVID-19 pandemic of 2020 is, however, unique in that advances in information and communications technologies have enabled business and government datasets to be monitored and mined to see how some types of economic crime changed over the duration of the pandemic. Moreover, there has been more systematic and public concern about fraud and online scams affecting the community from the beginning of the COVID-19 pandemic. Monitoring of fraud trends is not, however, as mature as monitoring of infection rates and deaths caused by the COVID-19 virus, although the extent of baseline information on the impact of fraud is much better than in respect of any previous global event. As such, some data relevant to changes in the prevalence of fraud now exist, albeit in sometimes overly general form.

Although the precise extent of fraud arising from the COVID-19 pandemic in 2020 will not be known for some time—indeed, a proportion of this fraud may never be identified or quantified, depending on the risk appetite and tolerance of governments—it is clear that the fiscal and social changes that have taken place have created abundant opportunities for acts of dishonesty and fraud to occur. Whether the financial benefits of prompt implementation of stimulus and support measures outweigh the risks of financial crime remains to be seen. It is likely, however, that a proportion of the many billions of dollars (and pounds) at stake will be lost to fraud.

What is surprising is that during the first nine months of the current pandemic, identified fraud has been relatively low. Losses due to identified government stimulus fraud, consumer scams and payment fraud have accounted for millions rather than billions. Arguably, many individuals and businesses might not have experienced the full economic impact of COVID-19 during 2020, having been supported by personal savings and government support programs. As the full impact of the pandemic is felt, it is likely that the cost of fraud will increase considerably.

Best practice in preventing fraud in future pandemics and economic crises

Bearing these limitations in mind, in what ways can governments, business and the community take action to minimise the risks of economic crime and fraud during pandemics and economic crises? 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 economic crises and 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 crises 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 (2020) also provides guidance on counter-fraud activities recommended for entities during the pandemic.

In the United Kingdom, 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 a five percent reduction in the number of all crimes between February and March 2020. Comparisons between April 2019 and April 2020 showed that 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 (686,000 to 632,000 incidents) and a 57 percent increase in computer misuse (299,000 to 468,000 incidents; Office of National Statistics 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 to fraud control 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.

In connection with fraud control, 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

Governments and business also 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, clear rules need to be in place to ensure that people who may be likely to act dishonestly 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, such that others in the community would be disadvantaged. 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 economic shocks and pandemics. Ideally, the nature and extent of fraud that occurred in previous crises need to be documented and understood so that similar risks can be avoided in the future. Although each crisis 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. 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: 76).

References

URLs current as at February 2021

Action Fraud (AF) 2020. UK Finance reveals ten Covid-19 scams the public should be on high alert for. London: Action Fraud. https://www.actionfraud.police.uk/news/uk-finance-reveals-ten-covid-19-scams-the-public-should-be-on-high-alert-for

Aliber A & Kindleberger C 2015. *Manias, panics, and crashes*, seventh ed. London: Palgrave Macmillan

Andon P & Free C 2020. Strain, coping and sustained fraud offending. *Trends & issues in crime and criminal justice* no. 596. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi596

Arnold C 2018. *Pandemic 1918: Eyewitness accounts from the greatest medical holocaust in modern history.* London: St Martin's Publishing Group

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

Attorney-General's Department 2020. *Counter fraud during the COVID-19 pandemic.* Canberra: Attorney-General's Department. https://www.ag.gov.au/integrity/counter-fraud/counter-fraud-during-covid-19-pandemic

Australian Bureau of Statistics (ABS) 2020. *Labour force, Australia.* ABS cat. no. 6202.0. Canberra: ABS. https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia

Australian Bureau of Statistics 2008. *Australian historical population statistics*. ABS cat. no. 3105.0.65.001. Canberra: ABS. https://www.abs.gov.au/statistics/people/population/historical-population

Australian Competition and Consumer Commission (ACCC) 2020. Current COVID-19 (coronavirus) scams. https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

Australian Competition and Consumer Commission (ACCC) 2009. Swine flu scams. Canberra: ACCC. https://www.scamwatch.gov.au/news-alerts/swine-flu-scams

Australian Cyber Security Centre (ACSC) 2020. COVID-19 cyber security advice. Canberra: ACSC. https://www.cyber.gov.au/acsc/services/covid-19-cyber-security-advice

Australian Government 2020. *Budget 2020–21*. https://budget.gov.au/2020-21/content/overview.htm

Australian Payments Clearing Association (APCA) 2014. Payment fraud statistics—Jul 2013 to Jun 2014. Sydney: APCA. https://www.auspaynet.com.au/insights/fraud-statistics/2014-FinancialYr

Australian Payments Network (AusPayNet) 2020a. *Australian payment fraud 2020*. Sydney: AusPayNet. https://www.auspaynet.com.au/resources/fraud-statistics/2019-Calendar-year

Australian Payments Network (AusPayNet) 2020b. Cash payments network. Sydney: AusPayNet. https://www.auspaynet.com.au/network/cash

Australian Payments Network (AusPayNet) 2019. *Australian payment card fraud 2019*. Sydney: AusPayNet. https://www.auspaynet.com.au/resources/fraud-statistics/2018-Calendar-year

Australian Securities and Investments Commission 2020. Insolvency statistics – Series 1B: Notification of companies entering external administration. Chart 1B.3. https://asic.gov.au/regulatory-resources/find-a-document/statistics/insolvency-statistics/insolvency-statistics-series-1b-notification-of-companies-entering-external-administration-weekly-update/

Australian Taxation Office (ATO) 2020a. Phoenix taskforce. Canberra: ATO. https://www.ato.gov.au/general/the-fight-against-tax-crime/our-focus/illegal-phoenix-activity/phoenix-taskforce/

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

Balleisen E 2017. *Fraud: An American history from Barnum to Madoff*. Princeton: Princeton University Press

Bell RE 2004. The seizure, detention and forfeiture of cash in the UK. *Journal of Financial Crime* 11(2): 147

Berger K 2020. Shady landlords and bootleggers ruled Seattle's last pandemic. *Crosscut*, 7 April. https://crosscut.com/2020/04/shady-landlords-and-bootleggers-ruled-seattles-last-pandemic

Blinder M 2014. *What did we learn from the financial crisis, the great recession, and the pathetic recovery?* Working Paper no. 243. Princeton: Griswold Center for Economic Policy Studies

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

Braithwaite J 1989. *Crime, shame & reintegration*. Cambridge: Cambridge University Press

Broadhurst R, Ball M & Jiang CJ 2020. *Availability of COVID-19 related products on Tor darknet markets*. Statistical Bulletin no. 24. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sb/sb24

Buffett W 2018. Who has been swimming naked? Letter to Berkshire-Hathaway shareholders on 29 April 2007. *Buffettpedia*, 29 April. http://buffettpedia.com/2018/04/who-has-been-swimming-naked/

Cabinet Office 2020. *Government functional standard GovS 013: Counter fraud: Counter fraud, bribery and corruption*. London: HM Government. https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud

Caddy J, Delaney L, Fisher C & Noone C 2020. Consumer payment behaviour in Australia. Sydney: Reserve Bank of Australia. https://www.rba.gov.au/publications/bulletin/2020/mar/consumer-payment-behaviour-in-australia.html

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. https://www.dailymail.co.uk/money/markets/article-8653807/Fraudsters-raid-Chancellor-Rishi-Sunaks-loan-fund.html

Canberra Times 1991. $50m in Newcastle earthquake fraud. 21 September. https://trove.nla.gov.au/newspaper/article/122385439

Canberra Times 1974. Flood relief fraud. 13 February. https://trove.nla.gov.au/newspaper/article/110761258

Canberra Times 1964. Voyager fraud alleged. 25 February. https://trove.nla.gov.au/newspaper/article/131745255

Carnegie GD & O'Connell BT 2014. A longitudinal study of the interplay of corporate collapse, accounting failure and governance change in Australia: Early 1890s to early 2000s. *Critical Perspectives* on *Accounting* 25(6): 446–68

Carswell AT & Bachtel DC 2009. Mortgage fraud: A risk factor analysis of affected communities. *Crime, Law and Social Change* 52(4): 347–64

Cash Essentials 2020. Coronavirus: Beware of cash scams. *Cash Essentials*, 29 March. https://cashessentials.org/news/coronavirus-beware-of-cash-scams/

Cavaglieri C 2020. Fraud victims refused a refund are urged to ask financial ombudsman for review. *Which?* 1 April. https://www.which.co.uk/news/2020/04/fraud-victims-refused-a-refund-urged-to-ask-financial-ombudsman-for-review/

Cialdini R 2009. *Influence: The psychology* of *persuasion*, revised ed. New York: HarperCollins

Cifas 2020. *Fraudscape 2020*. London: Cifas

Cifas 2019. *Fraudscape 2019*. London: Cifas

Cifas 2011. *Fraudscape 2011*. London: Cifas

Cifas 2009a. Cifas fraud threat assessment 2009–2010 [unpublished]

Cifas 2009b. *The anonymous attacker.* London: Cifas

Clarke RV 2012. Opportunity makes the thief. Really? And so what? *Crime Science* 1: 3–9. https://doi.org/10.1186/2193-7680-1-3

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

Clinard MB 1952. *The black market: A study of white collar crime.* New York: Rinehart & Co, Inc

Competition and Markets Authority (CMA) 2020. Joint statement against price gouging. https://www.gov.uk/government/publications/cma-and-trade-bodies-joint-statement-against-price-gouging/joint-statement-against-price-gouging

Cooper DJ, Dacin T & Palmer D 2013. Fraud in accounting, organizations and society: Extending the boundaries of research. *Accounting, Organizations and Society* 38: 440–457

COVID-19 Hotel Quarantine Inquiry 2020. *Final report*. Melbourne: Victorian Government Printer. https://www.quarantineinquiry.vic.gov.au/reports

Crooks E 2017. More than 100 jailed for fake BP oil spill claims. *Financial Times*, 15 January. https://www.ft.com/content/6428c082-db1c-11e6-9d7c-be108f1c1dce

Cross C 2020. Beware of bushfire scams: How fraudsters take advantage of those in need. *The Conversation*, 17 January. https://theconversation.com/beware-of-bushfire-scams-how-fraudsters-take-advantage-of-those-in-need-129549

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

Daily Mail 2018. 14 charged, 11 jailed: The full extent of Grenfell Tower fraud claims. *Daily Mail*, 24 August. https://www.dailymail.co.uk/news/fb-6091399/Who-convicted-Grenfell-Tower-frauds.html

Daly T 2019. China vows to tackle dead pig scam amid swine fever epidemic. *Reuters*, 12 July. https://www.reuters.com/article/us-china-swinefever/china-vows-to-tackle-dead-pig-scam-amid-swine-fever-epidemic-idUSKCN1U71CN?il=0

Daugherty G 2020. Talking to the dead: How the 1918 pandemic spurred a spiritualism craze. *History*, 21 April. https://www.history.com/news/flu-pandemic-wwi-ouija-boards-spiritualism

Davis B 2009. What's a global recession? *Wall Street Journal*, 22 April. https://blogs.wsj.com/economics/2009/04/22/whats-a-global-recession/

Department of Health 2020. Coronavirus (COVID-19) current situation and case numbers. Canberra: Department of health: https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert/coronavirus-covid-19-current-situation-and-case-numbers

Doig A & Levi M 2020. Editorial: The dynamics of the fight against fraud and bribery: Reflections on core issues in this PMM theme. *Public Money & Management* 40: 5, 343–48

Dupont B 2019. The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity* 5(1): 1–17. DOI: 10.1093/cybsec/tyz013

Economist 2017. Hurricanes provide plenty of opportunities for scams. *The Economist*, 14 September. https://www.economist.com/united-states/2017/09/14/hurricanes-provide-plenty-of-opportunities-for-scams

Ellis M 2018. 10 facts about crime on the home front in the Second World War. https://www.historyextra.com/period/second-world-war/10-facts-about-crime-on-the-home-front-in-the-second-world-war/

Ernst & Young 2016. *14th global fraud survey*. London: Ernst & Young

European Central Bank (ECB) 2020. *ECB payment statistics: United Kingdom, September 2020*. https://sdw.ecb.europa.eu/reports.do?node=1000001960

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

Europol 2017. *Serious and organised crime threat assessment: Crime in the age of technology*. The Hague: Europol. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol 2006. *EU organised crime threat assessment 2006.* The Hague: Europol

Fair L 2020. FTC, FDA warn companies making coronavirus claims. https://www.ftc.gov/news-events/blogs/business-blog/2020/03/ftc-fda-warn-companies-making-coronavirus-claims

Farrall S & Karstedt S 2020. *Respectable citizens: Shady practices*. Oxford: Clarendon Press

Felbab-Brown V 2020. Order from chaos: What coronavirus means for online fraud, forced sex, drug smuggling, and wildlife trafficking. Brookings, 3 April. https://www.brookings.edu/blog/order-from-chaos/2020/04/03/what-coronavirus-means-for-online-fraud-forced-sex-drug-smuggling-and-wildlife-trafficking/

Federal Trade Commission (FTC) 2020. Coronavirus advice for consumers. https://www.ftc.gov/coronavirus/scams-consumer-advice

Finlay R, Staib A & Wakefield M 2018. *Where's the money? An investigation into the whereabouts and uses of Australian banknotes*. Research Discussion Paper 2018–12. Sydney: Reserve Bank of Australia. https://www.rba.gov.au/publications/rdp/2011-2020.html

FINRA 2020. Investor alert: Bird flu stock scam could be hazardous to your financial health. https://www.finra.org/investors/alerts/bird-flu-stock-scam-could-be-hazardous-your-financial-health

Fligstein N & Roehrkasse AF 2016. The causes of fraud in the financial crisis of 2007 to 2009: Evidence from the mortgage-backed securities industry. *American Sociological Review* 81(4): 617–643

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

Fox L 2003. *Enron: The rise and fall*. New York: John Wiley & Sons

Frailing K & Harper DW 2017. *Toward a criminology of disaster: What we know and what we need to find out*. New York: Springer

Franks C & Smith RG 2020. *Identity crime and misuse in Australia: Results of the 2019 online survey.* Statistical Report no. 29. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr29

Geraldton Advertiser 1903. Gigantic fraud. 11 December. https://trove.nla.gov.au/newspaper/article/252832814

Giommoni L 2020. Why we should all be more careful in drawing conclusions about how COVID-19 is changing drug markets. *International Journal of Drug Policy* 83. https://doi.org/10.1016/j.drugpo.2020.102834

Government Counter Fraud Function 2020. *Fraud control in emergency management: COVID-19 UK government guidance*. London: UK Government. https://www.gov.uk/government/publications/fraud-control-in-emergency-management-covid-19-uk-government-guide

Graber C 2007. Snake oil salesmen were on to something. *Scientific American*, 1 November. https://www.scientificamerican.com/article/snake-oil-salesmen-knew-something/

Grabosky PN 1977. Sydney in ferment: Crime, dissent and official reaction, 1788 to 1973. Canberra: Australian National University Press

Gray KR, Frieder LA & Clark Jr GW 2005. *Corporate scandals: The many faces of corporate greed*. St Paul: Paragon House

Gregory J 2019. Four more charged over fraud in Grenfell Tower tragedy. *London News Online*, 21 November. https://londonnewsonline.co.uk/four-more-charged-over-fraud-in-grenfell-tower-tragedy/

Grenfell Tower Inquiry 2019. *Grenfell Tower Inquiry: Phase 1 report.* London: Her Majesty's Stationery Office. https://www.grenfelltowerinquiry.org.uk/phase-1-report

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

Health Administration Degree Programs 2020. 10 evil vintage cigarette ads promising better health. https://www.healthcare-administration-degree.net/10-evil-vintage-cigarette-ads-promising-better-health/

Healthy with Honey 2020. 'COVID-19'. https://healthywithhoney.com/category/covid-19/

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

Hendry J 2020b. ATO to match data for early access super scheme, JobKeeper crackdown. *IT News*, 23 June. https://www.itnews.com.au/news/ato-to-match-data-for-early-access-super-scheme-jobkeeper-crackdown-549600?eid=3&edate=20200629&utm_source=20200629_PM&utm_medium=newsletter&utm_campaign=daily_newsletter

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

Hickey P 2020. Federal officers raid High Wycombe home over woman's alleged superannuation fraud which officials say netted her thousands of dollars. *Perth Now*, 23 May. https://www.perthnow.com.au/news/wa/federal-officers-raid-high-wycombe-home-over-womans-alleged-superannuation-fraud-which-officials-say-netted-her-thousands-of-dollars-ng-b881556152z

HM Treasury 2020. HM Treasury coronavirus (COVID-19) business loan scheme statistics. London: HM Treasury. https://www.gov.uk/government/collections/hm-treasury-coronavirus-covid-19-business-loan-scheme-statistics

Hollow M 2015. *Rogue banking: A history of financial fraud in interwar Britain*. Basingstoke: Palgrave Macmillan

Houlbrook M 2016. *Prince of tricksters: The incredible true story of Netley Lucas, gentleman crook*. Chicago: Chicago University Press

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

IDCARE 2020. Homepage. https://www.idcare.org

IFW Global 2014. Aussie MH17 plane crash victims exploited on Facebook. https://www.ifwglobal.com/news-old/aussie-mh17-plane-crash-victims-exploited-on-facebook/

Jackman T 2017. Fraud inevitably follows disasters, so authorities in Texas, Florida prepare for post-storm scams. *Washington Post*, 9 September. https://www.washingtonpost.com/news/true-crime/wp/2017/09/08/fraud-inevitably-follows-disasters-so-authorities-in-texas-florida-prepare-for-post-storm-scams/

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

Jones MJ 2010. *Creative accounting, fraud and international accounting scandals*. John Wiley & Sons

Keller MH & Lorenz T 2020. Coronavirus spurs a wave of suspect websites looking to cash in. *New York Times*, 24 March. https://www.nytimes.com/2020/03/24/business/coronavirus-ecommerce-sites.html

Kerstein FA 2006. An overview of post-disaster fraud. *St Thomas Law Review* 18(3): 791–802

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

Kiersz A 2019. This chart shows every recession the US has gone through since 1960, and how they compare to the economic meltdowns of other countries. *Business Insider*, 16 August. https://www.businessinsider.com/chart-number-of-recessions-in-us-around-the-world-2019-8?r=US&IR=T

King R & Shen A 2020. Will cash survive Covid-19? Central Banking, 20 March. https://www.centralbanking.com/central-banks/currency/7509046/will-cash-survive-covid-19

King & Spalding LLP 2020. COVID-19 survey of federal and state price gouging laws. https://www.kslaw.com/pages/covid-19-survey-of-federal-and-state-price-gouging-laws

Levi M 2009. Suite revenge? The shaping of folk devils and moral panics about white-collar crimes. *British Journal of Criminology* 49 (1): 48–67

Levi M 2008. *The phantom capitalists: The organisation and control of long-firm fraud*, 2nd ed. Andover: Ashgate

Levi M 2006. The media construction of financial white-collar crimes. *British Journal of Criminology*, Special issue on markets, risk and crime, 46: 1037–57

Levi M 2002. Suite justice or sweet charity? Some explorations of shaming and incapacitating business fraudsters. *Punishment & Society* 4(2): 147–63

Levi M & 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* 26: 313–33

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* 67(1): 77–96

Levi M & Smith RG 2011. Fraud vulnerabilities and the global financial crisis. *Trends & issues in crime and criminal justice* no. 422. Canberra: Australian Institute of Criminology

Levi M & Soudijn M 2020. Understanding the laundering of organized crime money. *Crime & Justice* 49: 579–631

Mannheim H 1940. *Social aspects of crime between the wars.* London: Allen & Unwin

Marchione M 2009. FDA warns: Swine flu scams lurk on the internet. *Seattle Times*, 22 October. https://www.seattletimes.com/seattle-news/health/fda-warns-swine-flu-scams-lurk-on-the-internet/

Marsh P 2019. Combating the "flu": Spanish influenza in Ulster. http://historyhubulster.co.uk/spanishinfluenza/

Maurer D 2000. *The big con: The story of the confidence man*. London: Arrow

May T & Bhardwa B 2018. *Organised crime groups involved in fraud*. London: Palgrave

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. https://labourhistorycanberra.org/2018/06/the-spanish-influenza-pandemic-in-australia-1912-19/

Medicines and Healthcare Products Regulatory Agency (MHRA) 2020. Coronavirus: Global crackdown sees a rise in unlicenced medical products related to COVID-19. Media release, 19 March. https://www.gov.uk/government/news/coronavirus-global-crackdown-sees-a-rise-in-unlicenced-medical-products-related-to-covid-19

Modern Mississauga 2020. The history of how Mississauga's doctor McFadden quashed 'quack cures' for the Spanish Flu. 10 June. https://www.modernmississauga.com/main/2020/6/10/the-history-of-how-mississaugas-doctor-mcfadden-quashed-quack-cures-for-the-spanish-flu

Morton J & Lobez S 2011. *Kings of stings: The greatest swindles from Down Under*. Melbourne: Melbourne University Press

Mukherjee SK, Scandia A, Dagger D & Matthews W 1988. *Source book of Australian criminal and social statistics 1804–1988: Bicentennial edition*. Canberra: Australian Institute of Criminology

Nagelhout G, Hummel K, Goeij M, de Vries H, Kaner E & Lemmens P 2017. How economic recessions and unemployment affect illegal drug use: A systematic realist literature review. *International Journal of Drug Policy* 44: 69–83

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. https://www.ncsc.gov.uk/news/annual-review-2020

Newcastle Morning Herald and Miners' Advocate 1949. Gaol for flood relief fraud. 16 September. https://trove.nla.gov.au/newspaper/article/134168379

Office of National Statistics (ONS) 2020. Coronavirus and crime in England and Wales: August 2020. London: ONS. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/coronavirusandcrimeinenglandandwales/previousReleases

Organisation for Economic Co-operation and Development (OECD) 2020. Quarterly national accounts. https://stats.oecd.org/index.aspx?queryid=350#

Palmer-Derrien S 2020. 'Dob them in': Morrison lays down the law for employers thinking of pocketing the JobKeeper subsidy. https://www.smartcompany.com.au/coronavirus/warning-employers-jobkeeper-fraud/

Payments Journal 2020. Cybercriminals are using COVID-19 to commit fraud—Here's how to recognize them. https://www.paymentsjournal.com/cybercriminals-are-using-covid-19-to-commit-fraud-heres-how-to-recognize-them/

Poltz J 2020. Prosecutors arrest three in suspected Wirecard criminal racket. *IT News*, 23 July. https://www.itnews.com.au/news/prosecutors-arrest-three-in-suspected-wirecard-criminal-racket-550762

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. 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

Reinhart CM & Rogoff KS 2009. *This time is different: Eight centuries of financial folly*. Princeton: Princeton University Press

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/

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

Rodger J 2020. HMRC issues furlough fraud update as investigators probe 8,000 claims. *Birmingham Mail*, 11 August. https://www.birminghammail.co.uk/news/midlands-news/hmrc-issues-furlough-fraud-update-18749262

Roodhouse M 2013. *Black market Britain: 1939–1955*. Oxford: Oxford University Press

Ruiz D 2020. Coronavirus scams, found and explained. *Malwarebytes Blog*, 19 March. https://blog.malwarebytes.com/scams/2020/03/coronavirus-scams-found-and-explained/

Sante L 2000. Introduction. In D Maurer, *The big con: The story of the confidence man*. London: Arrow

Schuchter A & Levi M 2015. Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum* 39: 176–87

Services Australia 2020. Anti-fraud taskforce arrests two women on coronavirus, bushfire welfare fraud. Media release, 17 May. https://minister.servicesaustralia.gov.au/media-releases/2020-05-17-anti-fraud-taskforce-arrests-two-women-coronavirus-bushfire-welfare-fraud

Services Australia 2019. Taskforce Integrity. https://www.servicesaustralia.gov.au/organisations/about-us/taskforce-integrity

Shafer RG 2020. She posed as a nurse during the 1918 flu pandemic and went on a crime spree. *Washington Post*, 17 May. https://www.washingtonpost.com/history/2020/05/17/julia-lyons-spanish-flu-fake-nurse-1918-chicago/

Shore H 2015. *London's criminal underworlds, c. 1720 - c. 1930: A social and cultural history*. London: Palgrave Macmillan

Smith RG 1998. Plastic card fraud. *The Australian Banker* 112(3): 92–9

Smith RG 1994. *Medical discipline: The professional conduct jurisdiction of the General Medical Council 1858–1990*. Oxford: Clarendon Press

Smith RG & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey.* Research and public policy series no. 128. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/rpp/rpp128

Smithies E 1982. *Crime in wartime: A social history of crime in World War II*. London: Allen & Unwin

Snowden FM 2020. *Epidemics and society: From the Black Death to the present*. Yale: Yale University Press

Special Commission of Inquiry into the Ruby Princess 2020. *Report of the Special Commission of Inquiry into the Ruby Princess.* Sydney: NSW Government. https://www.nsw.gov.au/covid-19/special-commission-of-inquiry-ruby-princess

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. https://www.moneysavingexpert.com/news/2020/05/small-business-boost-as-bounce-back-loans-launched/

Stanford University 2020. Blowing smoke: Vintage ads of doctors endorsing tobacco. https://www.cbsnews.com/pictures/blowing-smoke-vintage-ads-of-doctors-endorsing-tobacco/

Stupp C & Rundle J 2020. Companies battle another pandemic: Skyrocketing hacking attempts. *Wall Street Journal*, 22 August. https://www.wsj.com/articles/companies-battle-another-pandemic-skyrocketing-hacking-attempts-11598068863

Sutton C 2020. Women charged over $27k COVID-19 JobSeeker Fraud. News.com.au. https://www.news.com.au/national/nsw-act/crime/women-charged-over-27k-covid19-jobseeker-fraud/news-story/b8549cac0d71061bac5a7926b2b9996d

Swanston T 2020. AFP arrest trio for trying to defraud coronavirus superannuation early access scheme. *ABC News*, 9 August. https://www.abc.net.au/news/2020-08-09/coronavirus-queensland-afp-arrests-superannuation-early-access/12530252

Sydney Mail and New South Wales Advertiser 1902. Kembla disaster. *Sydney Mail and New South Wales Advertiser*, 16 August. https://trove.nla.gov.au/newspaper/article/165381208

Sykes T 2010. *Six months of panic: How the global financial crisis hit Australia*. Sydney: Allen & Unwin

Sykes T 1994. *The bold riders: Behind Australia's corporate collapses*. Sydney: Allen & Unwin

Sykes T 1988. *Two centuries of panic: A history of corporate collapses in Australia*. Sydney: Allen & Unwin

Sykes GM & Matza D 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review* 22: 664–70. https://dx.doi.org/10.2307/2089195

Tett G 2009. Fool's gold: How unrestrained greed corrupted a dream, shattered global markets and unleashed a catastrophe. London: Little, Brown

Tew I 2020. HMRC cracks down on furlough fraud with first arrest. *FT Adviser*, 31 July. https://www.ftadviser.com/your-industry/2020/07/13/hmrc-cracks-down-on-furlough-fraud-with-first-arrest/

Thomas D & Megaw N 2020. Coronavirus accelerates shift away from cash. *Financial Times*, 27 May. https://www.ft.com/content/430b8798-92e8-4b6a-946e-0cb49c24014a

Thomas J 2015. Australians warned about Cyclone Pam scammers. *SBS News*, 17 March. https://www.sbs.com.au/news/australians-warned-about-cyclone-pam-scammers

Toms S 2019. Financial scandals: A historical overview. *Accounting & Business Research* 49(5): 477–499. DOI: 10.1080/00014788.2019.1610591

Tooze A 2019. *Crashed: How a decade of financial crises changed the world*. London: Allen Lane

Transform Justice 2020. Does virtual justice increase discrimination? London: Transform Justice. http://www.transformjustice.org.uk/does-virtual-justice-increase-discrimination/

Treasury 2020a. Economic response to the coronavirus. Canberra: The Treasury. https://treasury.gov.au/sites/default/files/2020-03/Overview-Economic_Response_to_the_Coronavirus_2.pdf

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

Treasury 2017. *Black Economy Taskforce: Final report*. Canberra: The Treasury. https://treasury.gov.au/review/black-economy-taskforce/final-report

UK Finance 2020a. *2020 half year fraud update*. London: UK Finance. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/2020-half-year-fraud-report

UK Finance 2020b. *Fraud: The facts 2020*. London: UK Finance. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2020

University of North Carolina at Chapel Hill (UNC) Libraries 2020. Going viral: Impact and implications of the 1918 flu pandemic. https://exhibits.lib.unc.edu/exhibits/show/going-viral/profiting

US Department of Justice 2020. National Center for Disaster Fraud. https://www.justice.gov/disaster-fraud

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

van Driel H 2019. Financial fraud, scandals, and regulation: A conceptual framework and literature review. *Business History* 61(8): 1259–1299

Vollet T 2020. During Spanish influenza, snake oil salesmen were selling their 'cures'. *Chillicothe Gazette*, 8 April. https://www.chillicothegazette.com/story/news/2020/04/08/spanish-flu-influenza-snake-oil-salesmen-selling-cure-ohio/5119794002/

Walker S 2020. COVID-19 and crime: A response develops at the UN. Geneva: Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/analysis/covid-19-un-response/

Wall Street Journal 2020. Coronavirus advice is everywhere: It was the same with the Spanish flu. *Wall Street Journal*, 12 June. https://www.wsj.com/articles/coronavirus-advice-is-everywhere-it-was-the-same-with-the-spanish-flu-11591974530

We Live Security 2014. MH17 plane crash victims exploited by cold-hearted scammers. https://www.welivesecurity.com/2014/09/10/mh17-plane-crash-scam/

Weekly Times 1939. Bogus bushfire victims. *Weekly Times*, 11 March. https://trove.nla.gov.au/newspaper/article/225576017

Weinland D, Jenkins P & Crow D 2019. USB was riding high in China – until Swinegate. *Financial Times*, 18 June. https://www.ft.com/content/5f97b860-9187-11e9-aea1-2b1d33ac3271

Welford J 2020. HMRC: The thousands of reports of alleged furlough fraud made since the scheme started. *Teesside Live*, 1 August. https://www.gazettelive.co.uk/news/teesside-news/hmrc-thousands-reports-alleged-furlough-18675353

World Health Organization (WHO) 2020. WHO coronavirus disease (COVID-19) dashboard. https://covid19.who.int/

Zinsser H 2000. *Rats, lice and history*, revised edition. London: Penguin Books

Zirkle J 2020. Coronavirus fraudsters add to the anxiety and misery. https://www.acfe.com/article.aspx?id=4295010402

AIC reports

Research Report

Professor Michael Levi is Professor of Criminology in the School of Social Sciences at Cardiff University, Wales.

Dr Russell G Smith is a Fellow and former Principal Criminologist at the Australian Institute of Criminology, and Professor in the College of Business, Government and Law at Flinders University.

Australia's national research and
knowledge centre on crime and justice

aic.gov.au