FRAUD ADVISORY PANEL

Running on empty

How the pandemic revealed a wasted decade

Covid fraud and Covid vaccine fraud

Source: NFIB, City of London Police

A strange new world

We didn't need a global pandemic to teach us that fraudsters prosper when everyone else is on the back foot. The greater the uncertainty, the easier fraudsters find it to take advantage. We've seen it over and over again.

The pandemic created an unprecedented confusion of unfamiliar ways to do familiar things – working, shopping, earning, caring, loving, living.

And most of them had to happen right there, in the fraudsters' playground – cyberspace.

The dramatic consequences are visible everywhere, in the crime figures and beyond.

> **'All learning needs to happen rapidly because of the likelihood of future pandemics.'**
>
> Science and Technology select committee, October 2021[1]

What the numbers tell us

With the streets quiet, pubs and bars closed, and homes occupied around the clock, vehicle theft, robbery, mugging, burglary and theft from homes all fell by about half.[2] Suspects also became much easier to locate and apprehend. Similar trends were found all over the world; the tougher the movement restrictions, the larger the decline.[3]

Fraud and cybercrime were a different story.[4] Fraudsters quickly adapted their techniques to exploit our pandemic anxieties, relative isolation and growing dependence on the internet. Across the two pandemic years of 2020 and 2021, self-identified fraud against individuals leapt by 41% (5.2m offences) and computer misuse more than doubled (1.8m).[5] The culprits remained as elusive as ever.

ORGANISED CRIME

The United Nations Office on Drugs and Crime (UNODC) saw that movement restrictions were hampering trafficking and smuggling, leading organised crime groups to infiltrate high-demand sectors like medical equipment, pharmaceutical products and e-commerce. The pandemic also provided an extraordinary PR opportunity: criminal gangs handed out food, sanitisers and pharmaceutical supplies to the needy in Italy, Mexico, Japan and South Africa (where they declared a temporary truce).[6]

FRAUD AGAINST THE GOVERNMENT'S ECONOMIC SUPPORT PACKAGE

One consequence of three national lockdowns to save lives and protect the NHS was a need to keep society solvent in the meantime.

On 17 March 2020 the Chancellor unveiled a financial support package worth £330bn and pledged to do 'whatever it takes'. His prime objective – to get money quickly into the hands of mothballed businesses and frightened people – would be met, but at the cost of breathtaking amounts of fraud.

- **The banks distributed generous government-backed loans.**
- **HMRC launched a scheme to pay 80% of salary for furloughed employees.**
- **Local authorities distributed a range of government-funded grants to local companies.[7]**

Official estimates of fraud relating to the support package are eye-watering: £4.3bn in the Bounce Back Loans (BBLs, which were 93% of all loans); £5.7bn in HMRC's three schemes; £1bn (or more) in the grants distributed by local authorities.

As the National Audit Office (NAO) noted – and we have repeatedly argued over the years – the various enforcement agencies now have a very limited capacity to investigate, prosecute and recover large-scale fraud. In the case of bounce-back fraud alone, by October 2021 the National Investigation Service (NATIS) had received more than 2,100 intelligence reports but had the capacity to pursue no more than 50 cases a year (2.4%).[8]

UNPROTECTED PPE

The pandemic procurement failings of the Department of Health and Social Security (DHSC) will cost the nation £9bn in total – almost half of it (£4bn) from unsuitable PPE now destined for destruction – with a quarter of all contracts still subject to dispute.[9]

Transparency International believes that one in five government PPE contracts could be tainted by corruption.[10] The government's 'VIP' PPE procurement lane, which bypassed fraud and anti-corruption safeguards, has been found illegal by the high court.[11]

The NAO has been told that the final figure for fraud and error in pandemic PPE procurement will be between 0.5% and 5%.[12]

Scrutinising the DHSC's long-overdue 2020/21 annual report, the Public Accounts Committee (PAC) says the department's failure to apply normal controls – including to conflicts of interest among senior figures – helped significantly to leave the department open to fraud and to aggravate losses to the taxpayer.[13]

Picking the public pocket

NO BLACK SWANS

Covid-19 was not a Black Swan event. It was not only foreseeable, it was foreseen. And not only by Bill Gates.[14]

Epidemiologists have long warned that the foundations of a deadly pandemic were being laid by all-too-common human activity: habitat destruction, the climate crisis, wildlife trafficking and the aggressive exploitation of nature. Something much worse, they say, is surely just around the corner.[15]

Pandemic risks have been included in the National Risk Register since 2008 (updated in December 2020).[16] A month before lockdown, the Cabinet Office issued guidance on effective fraud control in emergency management and recovery, saying: 'emergency relief and services has an inherently high risk of fraud, and is a prime target'; it would be a failure 'for fraud to happen in an uncontrolled manner, with the responsible leaders unaware'.[17]

A joint report of the House of Commons Science and Technology and Health and Social Care Committees has also made this point forcibly: the lessons from health emergencies involving SARs (2003), swine flu (2009), MERS (2012) and Ebola (2013), as well as the 2008 financial crisis (when support measures were also introduced in a rush with inadequate fraud controls[18]), could have been, and should have been, better learnt.[19]

So, while we recognise the urgency of supporting the economy by getting money out to those in need as quickly as possible, we do not accept that this crisis was unanticipated or that it could not have been better planned for.

CAUGHT NAPPING

The pandemic caught the UK with its institutional defences down.

- **An underfunded NHS was short of PPE, clinical skills and ICU capacity.[20]**
- **The criminal justice system was chronically underfed and overstretched.**
- **The infrastructure and capabilities of local government had been systematically hollowed out by more than a decade of underfunding.**
- **The benefit system had been rendered so inadequate compared to the needs of poor people that food banks are ubiquitous.[21]**
- **The civil service was shrunk, drained and distracted by Brexit.[22]**

The prospects of mounting an effective emergency response, with strong counter-fraud and anti-corruption principles at its core, were not good and hadn't been for many years.

DOWN – AND OUT?

The Criminal Justice System (CJS), like so much of the nation's defences, was on its knees long before the pandemic. As we have said so often over the years, the CJS (in spite of all the hard work and goodwill it commands) is entirely unable to provide anything like a satisfactory criminal justice response to victims of fraud and cybercrime. But to say it again now feels almost redundant since that depressing fact is today true for every category of crime.

The most recent Criminal Justice Joint Inspection found the whole function to have been under-resourced at the outset of the crisis and now struggling to recover. Some parts (particularly prisons, the Probation Service and crown courts) are operating at 'unacceptable levels'.[23]

The backlog of crown court criminal trials in England and Wales almost doubled to 59,928 in the 18 months to September 2021. The number of cases waiting longer than a year for trial has more than trebled since the pandemic began. Plans to tackle the problem have rightly been criticised by the Public Accounts Committee for their 'meagre ambition'.[24]

POLICE NUMBERS

In what feels like a tiny ray of hope in an otherwise bleak outlook for criminal justice, the government has promised to add 20,000 officers to the force by March 2023.[25] This would return numbers to approximately 2009 levels. A little more than half have already been recruited.

Of course, headline numbers have only ever been part of the story. There remains a serious shortage of experienced detectives and digital forensic specialists, which extra bodies alone cannot address.[26]

In 2021 the Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) revisited its 2018 report *Fraud: Time to choose*. The inspectors found that too little had changed in the intervening three years: investigation and prevention is still under-resourced and under-prioritised; not enough fraudsters are being caught and punished. While welcoming a three-year national policing strategy for tackling fraud, the inspectorate also found that short-notice, single-year budgets still make it hard to invest properly in intelligence, investigation and prevention.[27]

In cyber, HMICFRS was pleased to find more coordinated police thinking at the national level. But 43 separate local forces and a short-term approach to funding are working together to create unpredictable local experiences for victims and an inefficient national response to a threat which knows no geographical boundaries.[28]

POLITICAL WILL

Over the years evidence has accumulated that the main problem facing a wealthy and prosperous country like the UK is not a shortage of potential resources with which to fight fraud but a shortage of political will.

The speed of events since Russia invaded Ukraine on 24 February 2022 could barely have made that same point more eloquently. We welcome the overdue strengthening of the UK's money laundering and anti-corruption regulations – so long argued for by so many, and yet so frequently delayed.

FRAUD BY DESIGN IN PANDEMIC SUPPORT

The design of the stimulus packages created numerous opportunities – and incentives – for individuals to commit economic crime.[29]

This was not, as they say, 'rocket science'. Crisis responses to tropical cyclone disasters in Latin America, earthquakes in Italy and the 2011 tsunami in Japan were all blighted by organised crime groups preying on aid earmarked for things like distressed companies, medical and pharmaceutical supplies, hospital expansion and waste disposal.[30]

> **'When a government sets up new channels for public procurement or aid distribution in an emergency they should be monitored closely by people with the competence and experience to do it properly.'**
>
> **Michael Levi, Professor of Criminology, Cardiff University**

A straightforward fraud analysis would have anticipated much of the fraud now emerging in the pandemic support schemes.[31] It should have come as no surprise and could have been planned for.[32] Where the balance should lie between speed and precaution is such a fundamental question it should have been bottomed-out soon after the financial crisis and long before Covid struck.

In reality, oversight has been 'nothing less than woeful' and guilty of 'schoolboy errors', as we learnt from Treasury counter-fraud minister Lord Agnew when he resigned from the despatch box in January 2022.[33]

SO LITTLE DUE DILIGENCE, SO MUCH SELF-CERTIFICATION

Pre-pandemic the Government Counter Fraud Function (GCFF) put annual public sector fraud-and-error losses at between £29.3bn and £51.8bn. Its more recent review of 206 pandemic support schemes worth £387bn found 16 (£219bn) exposed to high or very high fraud risks. Many of the other 190 might be just as vulnerable but their risk assessments were insufficient to say for sure.[34]

Government-backed loans

We have not forgotten the urgency of the times. But it was also haste, along with poor planning and coordination, that created the gaping fraud vulnerabilities at the heart of the support package (and particularly BBLs). This concerned us (and others) right from the start.

A suite of four schemes, accessible only through high street and online banks, distributed a total of £80.37bn of loans.[35] The vast majority of them (93%, or 1.5m) were BBLs; 100% backed by the government, collectively

worth £47.36bn, and now somewhat infamous for the ease with which fraudsters could exploit the application process.[36]

In June 2020 the Panel together with Spotlight on Corruption and Transparency International collectively wrote to the Chancellor stressing the dangers of so little due diligence and so much self-certification. We urged him to publish borrowers' names to deter fraud and aid detection. We wrote to ministers again in August, this time proposing a central data repository (and governance structure) so that lenders could improve due diligence by sharing information. We made that proposal again to the Chancellor in February 2021.

The Panel was well placed to provide insight and support to the government in these matters. Our own Covid-19 Fraud Watch practitioner group met weekly from March 2020. We pooled intelligence on emerging threats and practical advice on prevention, then cascaded it through the public, private and third sectors.[37]

Spotlight on Corruption has since mounted a public interest challenge to the government's view that publishing the names of loan recipients would prejudice their (and other) commercial interests. The Information Commissioner ruled in favour of the government but admitted that the judgment was 'finely balanced'.

Spotlight on Corruption has appealed and the hearing (later in 2022) will also hear evidence from Lord Agnew and former Fraud Advisory Panel chairman David Clarke.

Getting-back bounce back

The Department for Business, Energy and Industrial Strategy (BEIS) and the British Business Bank (BBB) now think that between one-third and a half of all loans (most likely 37%, or £17bn) will be lost to fraud or insolvency. An initial fraud loss rate of about 11% (£4.9bn) has since been revised down to a still-hefty 7.5%.[38]

The Chancellor's 2021 Spring Statement included plans to turn the Cabinet Office counter-fraud function into the Public Sector Fraud Authority with a budget of £48.8m over three years.[39] Its job is to 'hold government departments to account for their counter-fraud performance, and help them identify fraud and seize fraudsters' money'.[40]

It is hard to see how such a relatively small sum could fund an appropriate response to such an enormous challenge.

In contrast, DWP losses increased sharply during 2020/21, reaching an all-time high of £6.3bn (3%), with about £2bn of it thought to be fraud.[41] The government's response has been to find £613m of extra funding over three years to pay for 2,000 specially trained specialists and expanded data analytics.[42]

'Furlough' and more

HMRC's pandemic support had three main strands. Furlough grants to employers covered 80% of wages, up to a maximum of £2,500 per person, and supported 11.7m jobs at a cost of £70bn.[43] Five rounds of the Self-Employment Income Support Scheme (SEISS) distributed another £28.11bn to sole traders and partnerships.[44] 'Eat Out to Help Out' provided meal subsidies worth £849m.[45]

HMRC estimates fraud and error in all three schemes at £5.8bn, the vast majority of it in furlough (loss rate 8.7%). Interestingly, losses for SEISS – no self-certification and HMRC calculated entitlements automatically using historic tax returns – are thought to be a more typical 2.5%, showing the value of tried and tested controls.[46]

Recovery prospects are (by HMRC's own calculations) slim indeed. Resource constraints have long hampered HMRC compliance work. In March 2021 the Chancellor promised an extra £280m for HMRC enforcement of one kind or another, including £100m for a 1,265-strong Taxpayer Protection Taskforce to tackle pandemic fraud.[47]

HMRC plans to recover just £2bn of the £5.8bn, £850m of which has already been gathered in. Only the most egregious abuse will be targeted, but how rigorously remains to be seen. The Public Accounts Committee thinks this target is 'unambitious' and an encouragement to future abuse. We agree. Fair taxes are the price we all should pay for a just society.[48]

By its own calculations HMRC generates £17 for every £1 it spends on compliance.[49] So we say it again: the business case for fraud detection and recovery is almost always compelling.

Minding the assurance gap in local government

Local government has been something of an unsung hero of central government's pandemic response.

A series of grant schemes, funded by central government but administered by local authorities – 4.5m individual payments worth £22.58bn – was the third key pillar of economic support.[50]

Here, uncertainty about governance, as well as long-standing fiscal tensions between central and local government, cast their shadow over much of the grant-making process.

> **'Our pre-payment checks were criticised at the time but they stopped some £12m of suspicious claims.'**
>
> Scott Warner,
> Counter-Fraud Manager,
> Oxford City Council

The amounts involved were vast by local government standards – for some councils almost equal to an entire year of normal spending[51] – and councils had little warning of, or assurance support for, the schemes they were expected to operate.

From the outset many councils wanted to use their local capabilities and knowledge to carry out pre-payment fraud checks. They were overruled. Speed was of the essence, they were told.

Guidance requiring councils to develop pre- and post-payment assurance systems for all grant schemes wasn't published until June 2020, more than two months after the first grants were issued.

Fearful that in spite of government assurances they might still be expected to cover fraud losses, some councils performed pre-payment fraud checks anyway. As one experienced council fraud officer wryly notes: 'Pay now – verify later? It simply doesn't work.'

When the government suddenly decided to encourage greater speed by publishing league tables of grant-making performance,[52] cautious councils found themselves roundly criticised for being at the bottom.

Pre-payment checks became mandatory in April 2021, but by then the three main schemes had closed and about half the money had already been distributed.[53] Councils found the government's National Fraud Initiative (NFI) platform for automated pre-payment checks far from automatic. Some councils gave up in frustration and paid for alternative systems from the private sector.

Hollowed-out

BEIS told the Public Accounts Committee's hearings on fraud and error that local authorities were probably better equipped than BEIS itself to handle fraud risks because they deal with them daily.[54]

In reality, councils' counter-fraud capabilities have been hollowed out over the past decade, accelerated by the transfer of housing benefit investigators to DWP in 2014. Where counter-fraud functions still exist, they largely fund themselves with recoveries and by selling their services.

Deep cuts in central funding and a real-terms freeze on council taxes cut local authority spending power by 29% between 2009/10 and 2019/20.[55] Covid has further

> **'The local government finance system is in crisis. Even pre-Covid we were seeing the audit market falling over and high-profile financial management failures from commercial investments that turned sour – all as local authorities desperately tried to make money and find savings to deliver essential services.'**
>
> Oliver Simms, Manager, Public Sector Audit and Assurance, ICAEW

impaired council budgets. An extra £10.4bn of central government funding to cover 2020/21 pandemic costs and revenue losses was short by £1.5bn.[56]

A BBC investigation into 170 upper-tier and single-tier UK councils struggling to recover from the pandemic found a £3bn black hole in their collective budgets.[57] Some are at real risk of bankruptcy and barely able to carry out their statutory duties.

Where are we now?

BEIS has looked at 0.05% of the three main grant schemes and estimated fraud and error at a best-guess of £1bn. Given the tiny sample and the very wide range of the estimate (between £514m and £1.56bn) this is surely too low.[58] And it does not include the remaining schemes: 3.5m individual grants worth £10.9bn.[59]

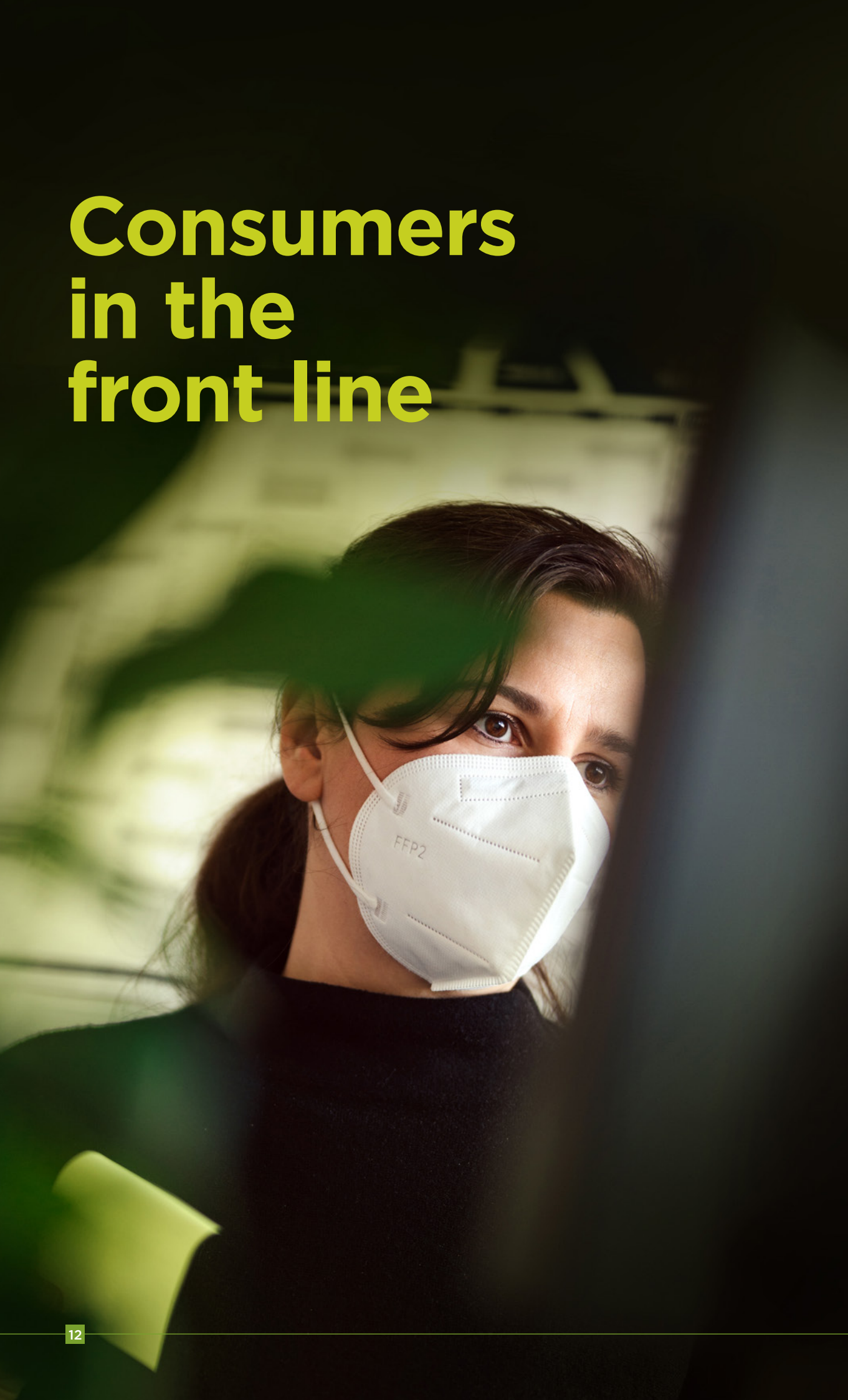
The government is now reviewing assurance arrangements and councils are currently responding to post-payment assurance questionnaires. Given everything we know about council resources and budgets, and about the tools and instructions they were given at the outset, these returns are likely to be variable in quality and timeliness.

The Panel believes that in meeting a national challenge the magnitude of Covid-19, local government should have been central government's trusted partner. Instead, councils tell us they found little understanding of what they do and the challenges they face.

A cross-sector counter-fraud authority – durable and well-funded enough to develop and mature in its role – is as badly needed at the local level as it is at the national level, as the Panel has consistently argued since the National Fraud Authority was disbanded in 2013. Local government will not form part of the Public Sector Fraud Authority's remit.

> **'We need a proactive cross-sector authority with the long-term funding to evolve and mature, and the power to require central government, local councils and other public bodies to work together whilst also pushing for legal changes to make counter-fraud data sharing and data access much simpler.'**
>
> Nick Jennings, Head of Service, Shared Anti-Fraud Service, Hertfordshire County Council

Consumers in the front line



A CYBER BLIZZARD

With most people driven indoors and increasingly dependent on the internet, fraudsters quickly adapted their pitches to pandemic themes.

Almost immediately the pandemic struck:

- **fake government emails offered Covid relief grants in exchange for personal information or help with Universal Credit applications for a fee paid in advance;**
- **fake contact-tracing alerts led people to fake websites designed to steal their data or spread malware;**
- **online adverts offered mail-order hand sanitiser and face masks which did not exist;**
- **scammers offered free TV licences, or warned of problems with direct debits or streaming subscriptions, or used fake dating profiles to manipulate the lonely and isolated;**
- **investment frauds and fake cryptocurrency opportunities urged people to get ahead of the coming recession.[60]**

We sometimes have the impression that fraud and cybercrime are now seen as a global fact of life. But data from fraud prevention technologists Seon, published by *The Financial Times*, reveals that internet fraud is in fact a problem that disproportionately harms people in the UK. For every French internet fraud victim there are 134 UK victims. For Germans the equivalent figure is 170. Even compared to other English-speaking countries, a UK resident is significantly more likely to fall victim to internet fraud: more than twice as likely as a US citizen; 22 times more likely than a Canadian; and 46 times more likely than an Australian.[61]

CRIME SURVEY OF ENGLAND AND WALES (CSEW)

The CSEW (the TCSEW from May 2020 when it became telephone-based) found that fraud increased by 41% and computer misuse more than doubled across the two pandemic years of 2020 and 2021.[62]

Meanwhile, consumer and retail fraud ballooned by three-quarters, and there was a truly staggering eleven-fold increase in advance fee frauds, many being parcel delivery scams.[63]

The biggest increase in cybercrime was unauthorised access to personal data – a combination of large-scale data breaches and hacking of email and social media accounts – up 174% to 1.5m offences.[64]

Slightly more than half of TCSEW respondents said they had received an online phishing communication within the previous month, many being pandemic themed. Just 3% admitted to having replied or clicked on the link.[65]

The National Cyber Security Centre's (NCSC) Active Cyber Defence programme took down 11,000 government-themed phishing scams. Most of them targeted pandemic anxieties and uncertainties by impersonating public bodies such as HMRC, the NHS, TV licensing and the DVLA.[66] Meanwhile, its Protective DNS – which stops malware already in circulation from calling home and activating itself – blocked more than 160m attempts.[67]

Widespread under-reporting makes police fraud and cybercrime data a poor indicator of overall trends. (TCSEW found that just one in four people report their phishing experiences, and then only rarely to their internet/phone provider or the NCSC.[68]) Even so, Action Fraud logged 15% more fraud offences in 2021, including 29% more financial investment frauds and 12% more advance fee frauds. UK Finance and Cifas referrals to the National Fraud Intelligence Bureau increased by 78% and 10%, respectively.[69]

CAUSE AND EFFECT?

Researchers at University College London mapped police crime data against mobility and online sales indicators. Online shopping fraud and hacking rocketed as soon as lockdown restrictions took hold.[70]

As each new lockdown came and went, online shopping fraud tracked the peaks and troughs of online sales. Hacking, on the other hand, did not show the same peaks for the second and third lockdowns.

Why would that be? Had internet users learnt lessons from the first lockdown? Or were we just less stressed once vaccines appeared on the horizon? (Covid-19 stress very likely left people less able to think rationally about other kinds of risk.)

Online sales quadrupled in the decade ending with 2021 and grew by 49.9% (to £113.2bn) in 2020 alone. Even though growth slowed in 2021 (to 8.7%) it remained positive.[71] And what applies for shopping also applies for online fraud and cybercrime; the trend will remain inexorably upward, with or without pandemics, unless we develop a much deeper understanding of the dynamics of victimisation, and what works in cybercrime defence and why.[72]

> **'Businesses have a duty to prevent scams from reaching their users and customers; they can and should intervene to disrupt the criminals. Equally, they should offer support and effective reporting processes for when their customers do fall victim.'**
>
> **Stephanie Borthwick,**
> **Senior Policy Adviser, Which?**

ONLINE SAFETY MUST GO FURTHER

Fraud and paid-for online adverts were belatedly included in the Online Safety Bill.[73] This is real progress, but regulation should cover adverts in search-engine results as well as those on social media platforms.

Which? rightly argues that building collective cybercrime resilience should primarily be a job for business and government organisations, not their customers.

TAKING RESPONSIBILITY

The individual's journey to victimisation includes many intermediate steps which will typically be provided, facilitated or controlled by legitimate companies that have security weaknesses in their systems, products and services.

Authorised push payment (APP) fraud is a case in point. It is only possible because of the way banks manage and control electronic payments. The government has finally moved to make APP fraud compensation mandatory.[74] Not before time; the most recent fraud update from UK Finance showed a 71% year-on-year increase in APP losses (to £355.3m) in the first half of 2021.[75]

Other examples of designed-in fraud vulnerabilities might include: how a mobile phone company manages customer SIM swaps; design failings that make official websites and messaging easy to spoof; the way some remote access software is designed; and, of course, the many steam-age obstacles put in the way of counter-fraud data sharing.

YOU … ARE THE WEAKEST LINK

Research by Which? in 2020[76] shed further light on why users need to be protected 'at source'. We are all prone to overconfidence and can be very poor judges of our own scam detection skills, especially online where our real-world instincts often let us down. Two-thirds of Facebook users were found to have limited understanding of scams, even less awareness of scam advertising and almost no grasp of how

things like interactive quizzes can be used to steal data and enable fraud. Very confident scam spotters were found in reality to be no better than anyone else.

LOSING SIGHT OF WELL-BEING

The extensive emotional and psychological injuries caused by fraud are often not captured by a headline fraud loss figure. Researchers have found that this is particularly true for investment fraud and identity theft victims. In the case of romance fraud (a crime that increased by 35% during the pandemic as criminals exploited lockdown loneliness and isolation[77]) some victims even show signs of post-traumatic stress disorder.[78]

Research by the Victims' Commissioner has found that almost a quarter of fraud victims (roughly 700,000 of them) fall into a 'high vulnerability' group, having lost significant sums and suffered severe emotional and psychological injury even when their losses were subsequently reimbursed.[79]

Harms like these are hard to quantify, but Which? has made a valiant effort.[80] A study looked at more than 17,000 CSEW responses (2017–20) and followed HM Treasury guidance to estimate the 'cost' to fraud victims of their lowered life satisfaction, poorer general health and raised anxiety. The results are compelling: an average of £2,509 lost by each victim, with 3.7m incidents of fraud in 2019–20 creating a total well-being loss of £9.3bn.

While welcoming expansion of the National Economic Crime Victim Care Unit, the Victim's Commissioner has noted that the service is not available in all police forces, and too many victims are still falling through the net. It is high time that a proper and complete understanding of fraud loss and harm is clearly incorporated into public policy and funding decisions, as well as into the counter-fraud and victim support responses of business.

IN THE FRONT LINE

The National Crime Agency calls 'online the new frontline'.[81] That's not hyperbole. Every day consumers fight in the new Information War,[82] often without realising and always with one hand tied behind their back.

The attack on Ukraine has shown how cyber (particularly fake news and disinformation) is a key part of modern hybrid warfare.[83] Europol reports many direct and indirect attempts by states to exploit the Covid-19 crisis for geopolitical ends.[84]

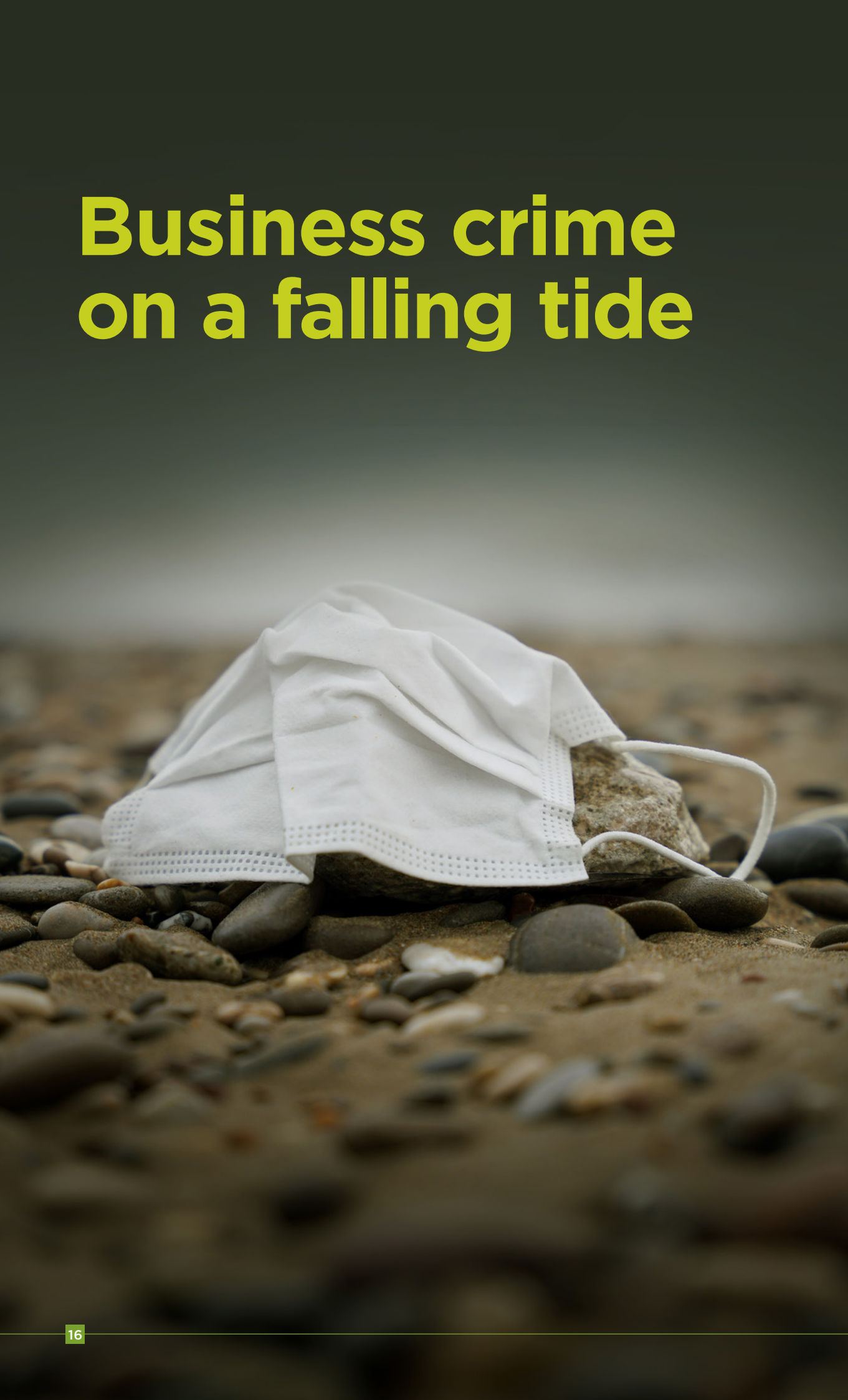
Meanwhile, social media influencers – some bad-faith actors, some 'useful idiots'[85] – can often be relied upon to lend them a hand. One 2021 study tracking anti-vaccine content found 65% of 812,000 Twitter or Facebook shares or reposts originated from just 12 public figures with large followings.[86]

GETTING SERIOUS

If we are serious about making the online space more secure for consumers, businesses, wider society and the national strategic interest, then:

- **there is no substitute for content identification, blocking and removal at source, by the platforms themselves;**
- **users who have engaged with fraudulent content by clicking or sharing should be warned individually;**
- **all social media platforms should be required to verify the identity of advertisers (and in the meantime flag suspect advertising content);**
- **there is an urgent need – as the Victims' Commissioner has said – for a quantum leap in both our understanding of fraud victims and their lived experiences, and in the availability and appropriateness of the support for them.[87]**

Business crime on a falling tide



BAD ON THE INSIDE

It is probably too soon to say what the pandemic has done to employee fraud inside organisations. Pandemic restrictions have hampered investigators' ability to interview, gather evidence and travel. And they are still adapting to a changed control and operating environment.[88] It will also take some time for the full consequences of working from home and the associated weakening of control, oversight and segregation of duties to emerge, but emerge they surely will.

Widespread evidence of deteriorating mental health and the ten-fold spike in state benefit claims as the first lockdown began[89] remind us that people were barely coping even before the cost-of-living crisis. Desperate people make bad decisions, whether they are trying to resist fraud or trying to resist the temptation to commit it.

Job moves reached record highs in 2021[90] making it the year of the Great Resignation (or rather the Great Reshuffle[91]). Movements of people between employers also carry the risk that corporate property – data and assets – will illegally move with them.

SWIMMING NAKED

The falling tide of recession often reveals economic wrongdoing. No longer kept afloat by a buoyant economy, fraudulent businesses and corrupt executives are finally seen (in Warren Buffett's memorable phrase) to be 'swimming naked'.

Two years of pandemic are likely to have made matters much worse this time. Hidden within the recent sharp spike in insolvencies[92] (monthly totals are running at twice the level of last year) there are believed to be a significant number of companies who dissolved themselves immediately after they received their Bounce Back Loans.

Insolvency Service investigations are continuing and prosecutions have begun. One involved a £30,000 loan paid to a company that had already ceased trading and been declared insolvent.[93] In another the company had been sold in 2019, and the £17,000 of pandemic support was used illegally to repay a family member.[94] Meanwhile a Glasgow-based company (with no identifiable legitimate business since January 2020) has been found to have lied to secure £240,000 of coronavirus loans.[95]

Cases like these are an increasingly common feature of post-pandemic insolvencies and practitioners expect them to snowball as insolvency numbers continue to grow. Low interest rates and banks chastened by their own failings in 2008 have together enabled a large number of zombie companies to hang on until the government's Covid-19 support package threw them another lifeline. Rising costs, including fuel prices and possibly interest rates, will finally signal the end of the road for many of them.

> **'It would have been very simple and virtually cost free to check whether a BBL applicant was filing dormant accounts at Companies House or had no real activity passing through its bank account.'**
>
> **Frances Coulson, Partner, Wedlake Bell LLP**

The United Nations Office on Drugs and Crime (UNODC) warns that desperate businesses can be forced into the arms of organised crime, creating a rich source of money-laundering opportunities and providing a gateway to government pandemic relief.[96]

The 100% government loan guarantee at the heart of the pandemic support package has injected these private risks into the heart of the public finances. As of 30 September 2021, BBB repayment data shows just 4% of BBLs by value (worth £2.04bn) fully paid back, 0.3% (£125.4m) in arrears and approximately 2.8% (£1.31bn) in default.[97]

YOUR MONEY OR YOUR LIFE

The pandemic created a rich pool of ransomware targets among hospitals, government departments, research facilities and critical manufacturing operations.

Most ransomware attacks seem to have used established tools (easily bought on the dark web) but new species did emerge frequently during the pandemic.[98] Delays between introduction/infection and activation have also grown shorter, as if the criminals feared this golden opportunity might soon pass.[99]

In an indication of the increased 'cyber-insider' threat to companies, Europol reports increased criminal efforts to actively recruit collaborators.[100]

Working from home and the e-commerce boom pushed internet capacity to the limits, creating many more opportunities for criminals to launch denial-of-service 'extortion' attacks against organisations and critical services.[101]

So-called 'double-extortion' attacks (in which criminals threaten to make public the data they have stolen or encrypted) have grown ten-fold since 2020, according to industry figures quoted by the NCSC.[102]

Over 3.1m malicious URLs were taken down by the NCSC in 2021 (1.4m in 2020), with much of the effort going into tackling extortion email campaigns (1.8m).[103]

One IT security specialist logged 1,243 large-scale data breaches in 2021, an 11% increase on 2020.[104] Pandemic data losses will haunt counter-fraud efforts for many years to come.

CARELESS WHISPERS

Recent rapid growth in the number and use of 'enterprise connected devices' (ECD) has created much additional vulnerability for many businesses. An ECD is often a laptop or smartphone, but it can also be any device designed to communicate with, store, or otherwise process an organisation's data, including corporate IoT (internet of things) devices, remote printers and data storage, even room-booking and video-conferencing systems.[105]

Our 2019 special report *Fraud Futures* noted the damage likely to be done by the careless corporate and consumer exploitation of IoT technology, expressing great concern about the consequences for fraud of a gathering tech tidal wave of AI, robotics, big data and more.

As this report attests, our collective cyber vulnerability has only grown since 2019 and was turbocharged by isolation, remote working and internet dependence during the pandemic. We can expect new and more intractable problems to emerge with each new phase of invention.[106]

Working from home increased these vulnerabilities substantially without many organisations fully realising, as staff performed sensitive data-intensive work at home unprotected by corporate firewalls and IT departments, and with controls lagging.[107]

A benchmarking exercise by the Association of Fraud Examiners (which ended in April 2021) had 1,539 responses, 7% of them from the UK. It found that: half of organisations have been finding more fraud since the pandemic began; three-quarters expect further growth post-pandemic; and 80% have changed at least one thing about their anti-fraud activities, with 40% having spent more on technology. Remote working and increased e-commerce activity were visible in the two-thirds who see changing business operations and consumer behaviour as their two biggest new risk factors.[108]

Lessons learnt, or simply deferred?

The pandemic posed a systemic threat. It found this country weakened by more than a decade of neglect of the public realm – policing, courts, hospitals, the civil service, local councils.

We must do better next time. But what should that mean? Our wish list includes:

Compulsory financial education (including fraud awareness) within all schools.

Companies required to design-out fraud vulnerabilities from their systems, products and services.

Policing reform to reflect the true harm caused by fraud, and funding commensurate with it.

A more systematic, thorough approach to counter-fraud checks across government and society.

Dismantling the obstacles to counter-fraud data-sharing – legal, institutional, political and commercial.

A better understanding of fraud victims' experiences and the support they need, as well as the funding to deliver it.

We welcome the government's forthcoming fraud strategy and hope that it will seek to address these issues and more.

The Covid-19 pandemic and the blizzard of cybercrime have, in a sense, the same root. They are both products of a new world in which everything and everyone is connected.

Only a holistic response can meet that challenge. We need to create a world that is resilient by design. That is the big lesson of the pandemic, in fraud and beyond.

End notes

[1] House of Commons Heath and Social Care, and Science and Technology Committees. (12 October 2021), *Coronavirus: lessons learned to date. Sixth Report of the Health and Social Care Committee and Third Report of the Science and Technology Committee of Session 2021-22*, HC 92.

[2] Office for National Statistics. (28 April 2022), *Dataset: Crime in England and Wales: Appendix Tables*.

[3] Nivette, AE., Zahnow, R., Aguilar, R. et al. (02 July 2021), 'A global analysis of the impact of COVID-19 stay-at-home restrictions on crime', *Nature Human Behaviour* 5, 868-877.

[4] Violent crime also increased. Police recorded more homicide (14%), domestic abuse (7%) and sexual offences (up 22% to the highest level ever recorded). See Office for National Statistics. (28 April 2022), *Crime in England and Wales: year ending December 2021*.

[5] Office for National Statistics. (28 April 2022), *Crime in England and Wales: year ending December 2021*.

[6] United Nations Office on Drugs and Crime. (July 2020), *The impact of COVID-19 on organised crime*, research brief.

[7] Browning, S. (27 January 2022), *Coronavirus: Business loans schemes*, House of Commons Library Research Briefing No. 8906.

[8] National Audit Office. (3 December 2021), *The Bounce Back Loan Scheme: an update*, press release.

[9] House of Commons Committee of Public Accounts. (10 June 2022), *Department of Health and Social Care 2020-21 Annual Report and Accounts: Sixth Report of Session 2022-23*, HC 253.

[10] Transparency International UK. (April 2021), *Track and Trace: Identifying Corruption Risks in UK Public Procurement for the Covid-19 Pandemic.*

[11] BBC News. (12 January 2022), *Covid: Government's PPE 'VIP lane' unlawful, court rules*.

[12] National Audit Office. (30 March 2022), *Investigation into the management of PPE contracts,* session 2021-22, HC 1144.

[13] House of Commons Committee of Public Accounts. (10 June 2022), *Department of Health and Social Care 2020-21 Annual Report and Accounts: Sixth Report of Session 2022-23*, HC 253.

[14] Ted. (2015), *The next outbreak? We're not ready.* Ted talk by Bill Gates.

[15] BBC Future. (14 January 2021), *Stopping the next one: What could the next pandemic be?*

[16] Cabinet Office. (2008), *National Risk Register*.

[17] International Public Sector Fraud Forum. (February 2020), *Fraud in Emergency Management and Recovery: Principles of Effective Fraud Control*.

[18] Levi, M., and Smith, RG. (2022), Fraud and pandemics. *Journal of Financial* Crime 29 (2), 413-432.

[19] House of Commons Heath and Social Care, and Science and Technology Committees. (12 October 2021), *Coronavirus: lessons learned to date. Sixth Report of the Health and Social Care Committee and Third Report of the Science and Technology Committee of Session 2021-22*, HC 92.

[20] The Kings Fund. (19 May 2022), *NHS funding: our position.*

[21] Boden, C. (23 March 2022), 'Rishi Sunak has broken his promise to help with the cost of living', *The Guardian*.

[22] Michael Savage. (17 November 2019), '*Stressed Whitehall staff at 'breaking point' over Brexit', The Guardian*.

[23] Criminal Justice Joint Inspection. (May 2022), *The impact of the Covid-19 pandemic on the criminal justice system – a progress report.*

[24] House of Commons Committee of Public Accounts. (9 March 2022), *Reducing the backlog in criminal courts. Forty-Third Report of Session 2021-22*, HC 643.

[25] Home Office. (30 March 2022), *National Statistics: Police workforce, England and Wales: 31 March 2021 second edition.*

[26] Criminal Justice Joint Inspection. (May 2022), *The impact of the Covid-19 pandemic on the criminal justice system – a progress report.*

[27] HMICFRS. (August 2021), *A review of 'Fraud: Time to choose' – A revisit of the 2018 fraud inspection to assess progress of the recommendations and areas for improvement*.

[28] HMICFRS. (October 2019), *Cyber: Keep the light on - An inspection of the police response to cyber-dependent crime*.

[29] Levi, M., and Smith, RG. (2022), Fraud and pandemics. *Journal of Financial* Crime 29 (2), 413-432.

[30] United Nations Office on Drugs and Crime. (July 2020), *The impact of COVID-19 on organised crime*, research brief.

[31] Levi, M., and Smith, RG. (2022), Fraud and pandemics. *Journal of Financial* Crime 29 (2), 413-432.

[32] Karvonen, K. (3 August 2020), 'How governments are combating Covid bailout fraud', *FT Adviser*.

[33] BBC News. (24 January 2022), *Conservative minister resigns in anger over Covid fraud.*

[34] House of Commons Committee of Public Accounts. (30 June 2021), *Fraud and Error. Ninth Report of Session 2021-22,* HC 253.

[35] Brien, P., and Keep, M. (29 March 2022), *Public spending during the Covid-19 pandemic*, House of Commons Library Number 09309.

[36] Hutton, G., and Keep, M. (16 May 2022), *Coronavirus business support schemes: Statistics*, House of Commons Library Research Briefing Number CBP 8938.

[37] House of Commons Committee of Public Accounts. *Written evidence submitted by the Fraud Advisory Panel* (to the Public Accounts Committee inquiry into fraud and error during the COVID-19 pandemic), FAE0002.

[38] National Audit Office. (3 December 2021), *The Bounce Back Loan Scheme: an update*, press release.

[39] Hinchliffe, R. (23 March 2022), 'Govt pours £48mn into new counter-fraud authority', *FT Adviser*.

[40] HM Treasury. (29 March 2022), *The Quiet Revolution: Redefining the 'How' of Government Spending*, speech by Chief Secretary to the Treasury, Simon Clarke MP.

[41] Department for Work and Pensions. (July 2021), *DWP annual report and accounts 2020 to 2021*, HC 422.

[42] Department for Work and Pensions. (May 2022), *Fighting Fraud in the Welfare System*, CP 679.

[43] Hutton, G., and Keep, M. (16 May 2022), *Coronavirus business support schemes: Statistics*, House of Commons Library Research Briefing Number CBP 8938.

[44] Ibid.

[45] Ibid.

[46] House of Commons Committee of Public Accounts. (11 February 2022), *HMRC Performance in 2020-2121. Thirty-Seventh Report of Session 2021-22*, HC 641.

[47] Wakeman, S. (1 July 2021), 'U.K. Tax Authority's Annual Report – Lessons to Be Learned?' *Bloomberg Tax*.

[48] House of Commons Committee of Public Accounts. (11 February 2022), *HMRC Performance in 2020-2121. Thirty-Seventh Report of Session 2021-22*, HC 641.

[49] Ibid.

[50] Department for Business, Energy and Industrial Strategy. (9 May 2022), *Coronavirus grant funding: local authority payments to small and medium businesses.*

[51] Department for Business, Energy and Industrial Strategy. (9 May 2022), *Coronavirus grant funding: local authority payments to small and medium businesses.*

[52] Jameson, H., and Peters, D. (17 April 2020), 'Government league table plan causes fury', *Local Gov*.

[53] Department for Business, Energy and Industrial Strategy. (May 2022), *Coronavirus grant funding: local authority payments to small and medium businesses.*

[54] House of Commons Committee of Public Accounts. (30 June 2021), *Fraud and Error. Ninth Report of Session 2021-22*, HC 253.

[55] House of Commons Committee of Public Accounts. (November 2021), *Written evidence submitted by Institute of Chartered Accountants in England and Wales (ICAEW),* LFS0001.

[56] Institute for Government. (January 2022), *Local authority costs incurred and income lost as a result of Covid-19 (2020/21 prices).*

[57] BBC News. (9 July 2021), *Covid leaves UK councils with £3bn financial black hole*.

[58] ICAEW. (14 February 2022), *BEIS Annual Report & Accounts 2020/21*, ICAEW Representation 16/22.

[59] Department for Business, Energy and Industrial Strategy. (9 May 2022), *Coronavirus grant funding: local authority payments to small and medium businesses.*

[60] UK Finance. (28 June 2020), *UK Finance reveals ten Covid-19 scams the public should be on high alert for*, press release.

[61] William Wallis. (31 May 2022), 'Policing needs reform to tackle UK's growing fraud problem', *Financial Times*.

[62] Office for National Statistics. (28 April 2022), *Crime in England and Wales: year ending December 2021*.

[63] Office for National Statistics. (28 April 2022), *Crime in England and Wales: Appendix table, Year ending December 2021 edition of this dataset.*

[64] Ibid.

[65] Office for National Statistics. (27 January 2022), *Nature of Crime: fraud and computer misuse, Year ending December 2021 edition of this dataset.*

[66] National Cyber Security Centre. (10 May 2022), *ACD The Fifth Year: Summary of Key Findings.*

[67] Ibid.

[68] Office for National Statistics. (28 April 2022), *Crime in England and Wales: coronavirus (Covid–19) and crime tables, Year ending December 2021 edition of this dataset.*

[69] Office for National Statistics. (21 July 2022), *Crime in England and Wales: year ending December 2021*.

[70] Shane D. Johnson & Manja Nikolovska. (15 March 2022), *The effect of COVID-19 restrictions on routine activities and online crime,* Dawes Centre for Future Crime, University College London.

[71] Office for National Statistics. (21 February 2022), *Online and instore retail sales, Great Britain, 2007 to 2021*.

[72] Shane D. Johnson & Manja Nikolovska. (15 March 2022), *The effect of COVID-19 restrictions on routine activities and online crime,* Dawes Centre for Future Crime, University College London.

[73] Department for Digital, Culture, Media and Sport and Home Office. (8 March 2022), *Major law changes to protect people from scam adverts online*, press release.

[74] HM Treasury. (10 May 2022), *New law to protect access to cash announced in Queen's speech*, news story.

[75] UK Finance. (22 September 2021), *2021 Half year fraud report*.

[76] Which? (14 October 2020), *Connecting the world to fraudsters- Report*, research report.

[77] Carter, E. (2021), 'Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud', *The British Journal of Criminology*, 16 (2), 283 -302.

[78] Whitty, M.T. and Buchanan, T. (2016), 'The online dating romance scam: The psychological impact on victims – both financial and non-financial', *Criminology & Criminal Justice*. 16 (2), 176–194, cited by Which? (November 2021), *Scams and Subjective wellbeing: Evidence from the Crime Survey for England and Wales*, research report.

[79] Poppleton, S., Lymperopoulou, K., and Molina, J. (October 2021), *Who suffers fraud? Understanding the fraud victim landscape*, Victims Commissioner.

[80] Which? (November 2021), *Scams and Subjective wellbeing: Evidence from the Crime Survey for England and Wales*, research report.

[81] National Crime Agency. (25 May 2021), *Online is the new frontline in fight against organised crime – says NCA on publication of annual threat assessment*, press release.

[82] Molander, RC., Riddile, A., and Wilson, PA. (1996), *Strategic Information Warfare: A New Face of War*, RAND Corporation.

[83] Cadwalladr, C. (6 March 2022), 'Social media turn on Putin, the past master'. *The Guardian*.

[84] Europol. (April 2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*.

[85] Perlman, D. (August 2019), *Hacking Ten Million Useful Idiots: Online Propaganda as a Socio-Technical Security Project*, Blackhat USA 50-minute briefings.

[86] Centre for Countering Digital Hate. (March 2021), *The Disinformation Dozen: Why platforms must act on twelve leading online anti-vaxxers.*

[87] Poppleton, S., Lymperopoulou, K., and Molina, J. (October 2021), *Who suffers fraud? Understanding the fraud victim landscape*, Victims Commissioner.

[88] Association of Certified Fraud Examiners and Grant Thornton. (2021), *The Next Normal: Preparing for a Post-Pandemic Fraud Landscape.*

[89] Department for Work and Pensions. (16 November 2021), *Official Statistics: Universal Credit statistics, 29 April 2013 to 14 October 2021.*

[90] Chartered Institute of Personnel and Development. (21 February 2022), 'The great resignation – fact or fiction?' *CIPD Voice*, 33.

[91] Christian, A. (14 December 2021), '*How the Great Resignation is turning into the Great Reshuffle*', BBC.

[92] The Insolvency Service. (17 May 2022), *Official Statistics: Commentary – Monthly Insolvency Statistics April 2022*.

[93] The Insolvency Service. (25 October 2021), *Insolvency Service cracks down on Bounce Back Loan abusers*, press release.

[94] Ibid.

[95] The Insolvency Service. (22 June 2021), *Insolvency Service takes action against businesses abusing COVID-19 financial support*, press release.

[96] United Nations Office on Drugs and Crime. (July 2020), *The impact of COVID-19 on organised crime*, research brief.

[97] British Business Bank. (Unknown), *Covid-19 emergency loan schemes repayment data*.

[98] Europol. (April 2020), *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*.

[99] Ibid.

[100] Ibid.

[101] Ibid.

[102] National Cyber Security Centre. (3 December 2021), *Weekly Threat Report 3rd December 2021.*

[103] National Cyber Security Centre. (May 2022), *Active Cyber Defence: The 5th Year: Summary of Key Findings.*

[104] Irwin, L. (20 January 2022), 'Data breaches and cyber attacks in 2021: 5.1 billion breached records', *It Governance*.

[105] National Cyber Security Centre. (10 May 2022), *Organisational use of Enterprise Connected Devices*.

[106] Fraud Advisory Panel. (July 2018), *Fraud Futures: Understanding the old to prepare for the new.*

[107] Deloitte. (Unknown), *Cyber crime – the risks of working from home.*

Acknowledgements

This report would not have been possible without the generous contributions of experts from across the counter-fraud community. The Panel extends its sincere thanks to everyone who agreed to be interviewed or otherwise contributed.

The Fraud Advisory Panel is the voice of the counter-fraud profession, committed to tackling fraud and financial crime. We aim to strengthen fraud resilience by championing best practice in fraud prevention, detection and response. We do this through education, advice and research.

Our members come from a wide range of professions and sectors and are united by their determination to counter fraud.

We were founded in 1998 by ICAEW which continues to support our work.

fraudadvisorypanel.org

FRAUD ADVISORY PANEL

Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA, UK
T +44 (0)20 7920 8721 E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Company Limited by Guarantee Registered in England and Wales No. 04327390
Charity Registered in England and Wales No. 1108863