BDO IDEAS | PEOPLE | TRUST

MAY 2021

FRAUD TYPOLOGIES – PARALLELING THE COVID-19 PANDEMIC

HOW FRAUDSTERS ARE USING COVID-19 POLICY ANNOUNCEMENTS TO TARGET YOUR BUSINESS

Following the World Health Organisation's (WHO) announcement of the COVID-19 pandemic on 11 March 2020, governments scrambled to protect their citizens from the potential fallout that COVID-19 could bring in its wake. The UK government implemented several of rapid and complex policy changes. These policies are covered in the press and published on the UK government website for the public to study and digest.

People and businesses alike struggled to manage complying with the numerous new COVID-19 policies, including three national lockdowns. We all experienced huge, and usually unwelcome, changes to our lives both at home and at work. However, these unprecedented changes have created huge opportunities for fraudsters that will have had them rubbing their hands together with delight.

You have probably experienced some of these opportunistic behaviours. A call from scammers claiming to be HMRC officials following up unpaid taxes and threatening to send bailiffs, a call supposedly from a well-known online retailer about failed payments and threatening to cut off services or an offer to help unclaimed government support.

We ask whether there is a relationship between the announcement of government policies and social measures related to COVID-19 and how fraudsters select and approach their targets.

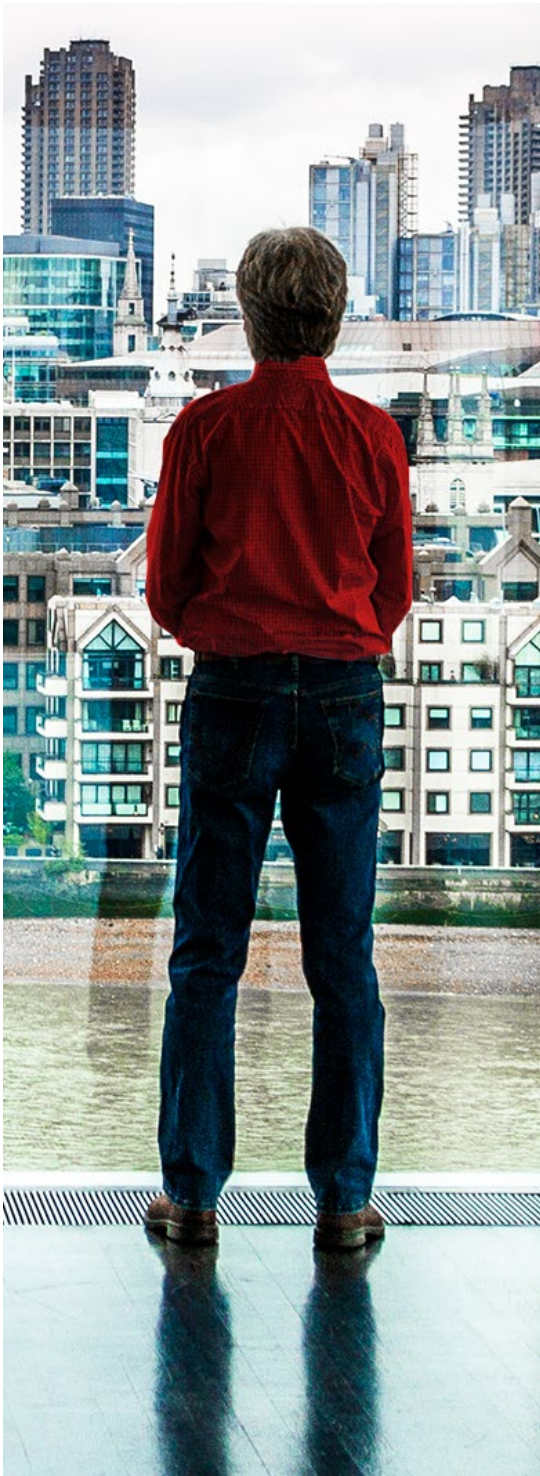
We will look at how fraudsters identify their targets and opportunities and whether it is possible to forecast or predict fraud.

The key data we examine is the National Crime Agency's Suspicious Activity Reports data and how they relate to government announcements and policy changes.

Finally, we explore how different types of fraud such as personal protection equipment (PPE) fraud, money laundering, government support programs fraud, investment fraud, private sector frauds and fraud against individuals have emerged or re-emerged since the COVID-19 policy announcements.

The final section of this report offers guidance on how those responsible for tackling fraud can better prepare for and prevent fraud against their businesses.

This report has been prepared by our forensic Senior Manager, Karen Edwards, using her academic and professional knowledge. It is an example of how we use that expertise to help our clients protect themselves and their businesses from fraud and other financial crimes.



HOW DO FRAUDSTERS DETERMINE THEIR NEXT TARGET OR OPPORTUNITY?

It could be argued that it is no different to criminals sussing out neighbourhoods to identify cars to steal – it is not random, it is calculated. Fraudsters are scanning the environment, looking for soft targets! The COVID-19 pandemic exploits human vulnerabilities and in the same way it highlights companies' vulnerabilities. With a blend of worsening social and economic conditions during the COVID-19 pandemic, there should be no doubt in anyone's mind that the plethora of resultant opportunities would lead to the emergence of increased levels of fraud.

The Association of Certified Fraud Examiners ("ACFE") estimates that organisations lose around 5% of revenue to fraud each year. ACFE 2020 Global Study on Occupational Fraud and Abuse, revealed that from the 2,504 cases studied, from 125 countries, there were losses of more than US$3.6 billion (more than £3 billion) from occupational fraud. ACFE's Benchmarking Report, September 2020 edition indicates that COVID-19's effect on fraud will contribute to an increase in global fraud well into 2021. This increase will likely be no different for UK organisations. A Financial Times article published in August 2020 reported that frauds against UK banking customers have increased by two-thirds. The UK government, HMRC and the Crown Prosecution Service have all issued alerts and warnings that fraudsters are exploiting the COVID-19 pandemic.

Fraudsters continue to take advantage of opportunities in the extended COVID-19 environment, including organisations' lack of preparedness and vulnerabilities. There have been reports by the Financial Times that fraudsters have stolen as much as £3 billion in the COVID-19 Job Retention Scheme alone to date.

It is irrefutable that fraudsters thrive on opportunities and experience shows that fraudsters may vary their techniques depending on the type of opportunities present. There should be no debate as to whether the current climate of the pandemic is rife with opportunities for fraudsters to exploit. But can these opportunities to some extent be mitigated by forecasting the fraudsters' next move?

FORECASTING FRAUD

It may be inconsistent or fractured thinking that makes us believe that frauds or fraud types cannot be forecasted. Paying close attention to the environment in which organisations are located and operate will prove that this is not necessarily the case. Whilst all future circumstances are not foreseeable, even when considering as many variables as possible, proactive continuous monitoring of your business environment will go a long way in fraud prevention. Fraudulent schemes are typically evolutionary not revolutionary.

It has been widely reported that the government's COVID-19 policies have resulted in unintended consequences. For example, the government's financial losses stemming from the new furlough scheme. While these consequences are unintentional, it does not mean they were impossible to forecast, detect, protect and prevent.

The government's COVID-19 policy announcements, have triggered new opportunities for fraudsters to exploit by highlighting targets that are directly and indirectly affected by these policies. Some organisations have become more vulnerable because they did not take the necessary preventative actions to mitigate their fraud risks. Fraud can be debilitating for businesses it can directly affect almost all areas of operations and because fraud losses incurred will not, in most circumstances, be recoverable.

SUSPICIOUS ACTIVITY REPORTS ("SARs")

Organisations within regulated sectors in the UK, such as financial institutions, are charged with reporting knowledge or suspicion of criminal activities as part of a reporting regime. This requires close monitoring of customers' activities. This section examines this reporting mechanism and how it has been used to monitor and record customer suspicious and/or fraudulent activities related to the COVID-19 pandemic between March 2020 and August 2020.

The National Crime Agency, circulated weekly Suspicious Activity Reports bulletins ("SARs data") setting out the types of fraud which have been prevalent during the COVID-19 pandemic. These have primarily been based on reports by banks who see transfers of money in real time. Each SARs bulletin summarises data related to COVID-19 related suspicious activity. SARs is the legislated reporting regime for financial institutions and other professionals to raise alerts about the knowledge or suspicion of criminal activities.

SARs data for the period 2 March 2020 to 9 August 2020 (inclusive) revealed that the number of SARs referencing COVID-19 increased from a weekly average of just over 20 in March 2020 to around 1,900 in July 2020, before it decreased to a weekly average of over 1,500 in August 2020. The graph below illustrates the weekly average number of SARs referencing COVID-19 from 9 March 2020 to 3 August 2020, no weekly information was available after this date.

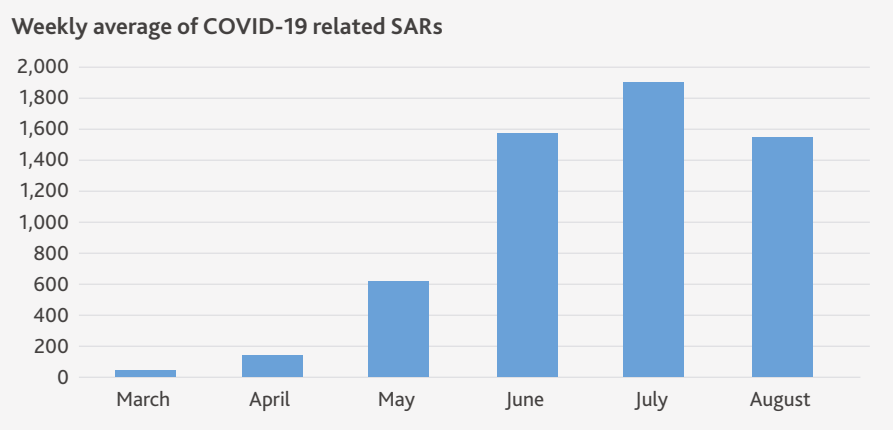


Figure 1: Average number of COVID-19 related SARs per week 9 March 2020 to 3 August 2020

The weekly percentage change in the number of these SARs are presented in the graphical illustration below.

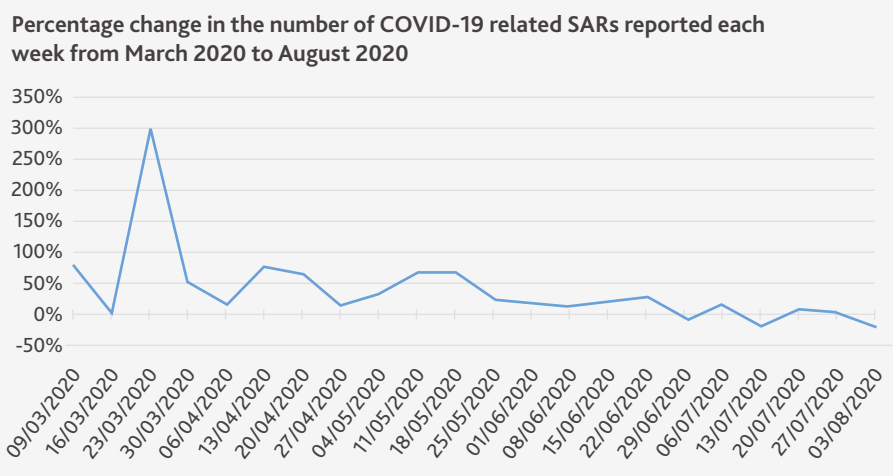


Figure 2: Percentage change in the number of COVID-19 related SARs reported weekly from 9 March 2020 to 3 August 2020

It can be observed from the graph that there was a sharp rise in COVID-19 related SARs in the week commencing 23 March 2020 when the first UK lockdown was announced, compared to the previous week. In the weeks that followed, there were week on week increases up to the week commencing 22 June 2020 until a slight decrease of around (8%) was observed in the week commencing 29 June 2020. Subsequent to this week, SARs continued to increase except for the weeks commencing 13 July 2020 and 3 August 2020, which recorded week on week decreases of (18%) and (20%), respectively.

GOVERNMENT'S COVID-19 POLICY ANNOUNCEMENTS AND SARs: OBSERVATIONS

Following the announcement of the COVID-19 pandemic, the government introduced policies that implemented several restrictions that affected business operations, schools, and the general public's activities. These included the requirement to **work from home** where possible and limiting social gatherings.

At the time of the first lockdown, the government established financial assistance schemes to ease some of the economic pressures that these restrictions created. As the pandemic ensued some restrictions were lifted or relaxed to enable economic and social activities to return to as normal as possible under the circumstances. The government kept the public apprised of each plan and timeline.

In this section, we consider how the government's COVID-19 policy announcements and launches may have had some effect on the types of fraudulent and potentially fraudulent activities reported in SARs.

To do this, the table below set outs the dates of some of the key government policy announcements, a summary extract of the new policy and mandated actions. This information is then compared with the information reported in weekly SARs data pertaining to potentially fraudulent activities identified.

These analyses consider other publicly available information around COVID-19, such as transcripts of the relevant government Ministers' speeches. These can be found on the UK government website and are hyperlinked to the date of each announcement.

DATE OF UK GOVERNMENT POLICY ANNOUNCEMENTS IN 2020	EXTRACTS FROM UK GOVERNMENT POLICY ANNOUNCEMENTS	SARs DATA
23 March	– UK lockdown announced – People were allowed to leave their homes for very limited purposes, including for essential travelling only – All social events stopped, and public gathering restricted to maximum two – Work from home (where possible) – Schools shut – all shops selling non-essential goods, shut – Coronavirus Business Interruption Loan Scheme (CBILS) launched – Coronavirus Job Retention Scheme (CJRS) announced – Self-Employment Income Support Scheme (SEISS) announced.	The week commencing 23 March saw the single largest percentage weekly increase in SARs related to COVID-19 for any week in the entire period reviewed, a 300% increase.
27 March 28 March 29 March 31 March	– Specific mention of Personal Protective Equipment (PPE) within government speeches and measures being taken to boost supply to protect frontline NHS – Establishment of National Supply Distribution Response Team to deliver equipment – Procurement of more ventilators from abroad – including from EU nations.	The week commencing 30 March, a week after first UK lockdown was announced, revealed the highest weekly reporting SARS volume to date, an increase of 53% on the previous week. This week's SARs data showed multiple reports of activities around customers purporting to sell face-masks and COVID-19 testing kits. There were also reports of legitimate websites being spoofed and being used as a conduit for selling PPE equipment.
1 April 3 April 13 April 20 April 29 April	– Business rate reliefs, smallest high streets firms grants, small business grants (SBGF) and funding for community pharmacies announced – CJRS went live – £300 million made available for funding community pharmacies – Securing more ventilators and PPE for NHS – PPE mentioned in almost all government speeches up to 29 April including that PPE was continuing to be sourced from home and abroad, including China, Myanmar and Turkey and to pursue every option available for PPE procurement – Future Fund convertible loan scheme for UK-based early stage companies launched – Innovate UK grant and loan funding launched.	The volume of SARs throughout the month of April continued to show weekly increases, with the highest increases recorded in the weeks commencing 13 April and 20 April (75% and 66%, respectively). There were a significant numbers of SARs relating to PPE fraud in the week commencing 20 April. These involved not only individuals but also companies. There were also a significant number of SARs that noted individuals and companies making overseas transfers for the purposes of obtaining PPE supplies. Also, there were notable rises in the number of SARs in respect of government priority schemes, primarily grants from local councils for small business relief. In the week commencing 27 April, SARs increased by 13%. Frauds involving the sale and purchase of PPE continue to be reported, some of which are large scale. SARs continued to report an increase in government priority scheme suspicious activities.

DATE OF UK GOVERNMENT POLICY ANNOUNCEMENTS IN 2020	EXTRACTS FROM UK GOVERNMENT POLICY ANNOUNCEMENTS	SARs DATA
4 May 10 May 13 May 18 May 29 May	– Bounce Back Loan Scheme (BBLS) launched – CJRS 4-month extension announced – SEISS launched – Advice to wear face coverings – SEISS extension announced: applications opening in August for a second and final grant.	68% weekly rise in SARs within weeks commencing 11 and 18 May, respectively. Two of the highest increases in weekly reports since COVID-19 related SAR reporting began.
4 June 15 June 23 June	– Face coverings to become mandatory on public transport as from 15 June – Non-essential shops including leisure venues re-open – secondary schools for year 10 and 12 pupils re–open – Announcement that from the 4 July pubs, restaurants etc. can reopen.	Large increases in SARs relating to face masks in weeks following. Continuing restrictions appear to result in an increase (38%) in cash based money laundering, in particular the week commencing 8 June. Following the re-openings of non-essential shops and some schools, the weeks commencing 15 and 22 June saw the SARs numbers remain consistent. In general, as shops reopen these numbers fall resulting in an (8 %) weekly decrease in SARs in week commencing 29 June.
9 July	– 4 July- Pubs reopen – 11 July- Outdoor performances allowed – 18 July- Local sports teams can play – 25 July- Gyms/leisure centres reopen.	In the weeks commencing 13 July and 3 August, weekly numbers of SARs reported reduced by (18%) and (20%) respectively, in particular for government priority schemes and PPE. Contrastingly, for the entire period from March through to the end of June, there was no single week where the number of reported SARs reduced.
24 July	– Face coverings became mandatory in shops and supermarkets.	For the week commencing 27 July, SARs directly classified as relating to PPE went up from 19 to 39 weekly reports, a 105% increase.

Sources: https://www.gov.uk/government/speeches and https://www.nationalcrimeagency.gov.uk/

From the table, it is seen that after the launch of certain government financial support programmes for businesses and individuals, potentially fraudulent activities around BBLS, SEISS, and CJRS contributed, sometimes significantly to the general increase of COVID-19 related SARs. This is particularly clear for the weeks commencing 23 March, 27 March, 11 May and 18 May 2020.

Similar trends were noted for frauds relating to PPE, supply chain, private sector and in some instances relating to individuals. In this case, for the weeks commencing 20 March, 20 April and 27 April 2020.

Further, it can be observed that in the weeks that certain restrictions eased and some business operations were re-opened or were returned to 'near-normal' conditions, there were reductions in the number of SARs referencing COVID-19. For example, this can be seen in the weeks commencing 29 June, 13 July and 3 August 2020.

Some additional observations made regarding the government's COVID-19 policy announcement and the possible correlation with the changes in the number of reports of potentially fraudulent activities are discussed below.

PERSONAL PROTECTION EQUIPMENT (PPE) RELATED FRAUDS

As more countries reported cases of COVID-19, there was an increased demand for PPE worldwide. On 3 March 2020 WHO announced that there was a worldwide shortage of PPE and UK frontline workers reportedly warned that PPE supplies were running low. There were reports in various UK media outlets around the **shortage of PPE** in the NHS. According to the BBC report on 12 June 2020, **"The availability of personal protective equipment (PPE) for health and care staff both before and during the Covid-19 pandemic has become one of the most intensely debated issues of the crisis"**. It became clear that PPE products were in high demand which, created opportunities for fraudsters.

The SARs data reviewed, first mentioned frauds relating to the procurement of masks in the week commencing 23 March 2020. It is seen that as PPE was mentioned in more speeches, SARs with specific mention of PPE related frauds increased. This increase was noticeable in the weeks commencing 28 March 2020 to 4 May 2020. Some of these reports mentioned a shift from small to larger scale procurement contract frauds regarding the acquisition of PPE.

In the week commencing 27 April 2020 there were reports of a possible multi-million pound fraud, where a medical supplies company appeared to knowingly inflate the price of PPE when securing a lucrative contract for its provisions. In this same week, the SARs data mentioned that there were several reports of financial institution's customers acting as middlemen by procuring deals for the provision of PPE despite not having any obvious affiliation to medical supplies provisions.

From the week commencing 18 May 2020 until week commencing 1 June 2020, as the mention of PPE in speeches lessened, there was a small decrease in the number of PPE related SARs reports. These numbers remained relatively constant until week commencing 29 June 2020.

Face coverings became mandatory on public transport and in shops on 15 June 2020 and 24 July 2020. PPE related reports doubled in the week commencing 6 July 2020. They increased again in the week commencing 13 July suggesting a possible link to increasing demand. This trend was observed despite the statement made by **Lord Deighton** to the BBC on 26 June 2020 that the PPE shortage crisis was over.

According to the SARs data reviewed, by the end of July 2020 to early August 2020, PPE frauds were primarily related to using the trade of PPE to cover up money laundering (discussed below) rather than PPE supply fraud.

It appears that fraudsters were exploiting opportunities arising from the increased demand for PPE supplies because of the government's policies, such as the mandatory requirement to wear masks on public transportation. It could be argued that fraudsters used the government's policy changes as a gauge to direct and time their attack.

There was comprehensive coverage in the press in respect of PPE frauds including conflicts of interests surrounding PPE procurement. For example, there was an instance where a **NHS official was investigated** in this regard.

MONEY LAUNDERING

Despite almost all shops selling non-essential foods and other premises being shut and the general public being advised to stay at home during the first national lockdown, the SARs data reviewed for the week commencing 23 March 2020 highlighted red flags for money laundering in respect of businesses exploiting the COVID-19 outbreak to cover up illicit movement of funds.

These types of red flags were also observed in the SARs data reviewed for the weeks that followed. For example some individuals claimed that they were sending funds abroad to family to purchase face masks. Also, large deposits in previously inactive accounts with claims that they were due to cancelled transactions and claims that funds received into accounts from multiple sources were from importing and selling masks.

One example of potential money laundering highlighted in SARs data in April 2020, was a horticultural business that had deposited close to £400,000 in cash since the start of the first UK lockdown. In this example, the business was still claiming to have made large cash sales despite not being allowed to trade.

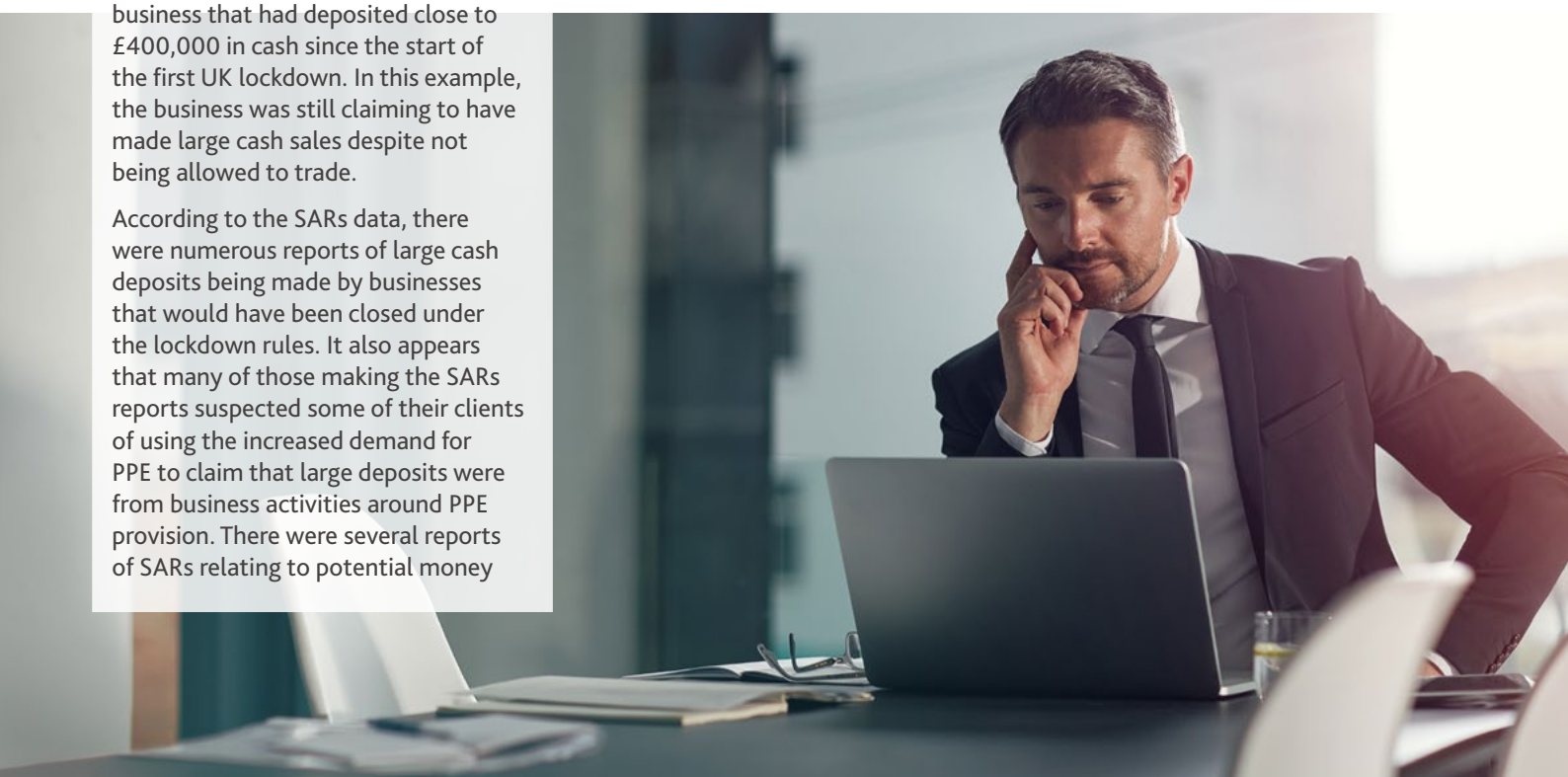
According to the SARs data, there were numerous reports of large cash deposits being made by businesses that would have been closed under the lockdown rules. It also appears that many of those making the SARs reports suspected some of their clients of using the increased demand for PPE to claim that large deposits were from business activities around PPE provision. There were several reports of SARs relating to potential money laundering by businesses relating to the PPE supply from the beginning of May 2020 to week commencing 8 June 2020.

SARs data reviewed show a slight decrease in the reports concerning the legitimacy of cash transactions in the week commencing 15 June 2020 when compared to the previous week. It appears that as non-essential shops reopened on 15 June 2020 and other restrictions eased, the number of SARs relating to COVID-19 and money laundering decreased. This arguably shows that potential fraudsters were adapting their behaviour in line with the changes in government's policies.

The Financial Action Task Force (FATF) produced a paper in May 2020 entitled **"COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses"**, that sets out amongst other things that:

- *"The increase in COVID-19-related crimes, such as fraud, cybercrime, misdirection or exploitation of government funds or international financial assistance, is creating new sources of proceeds for illicit actors.*
- *Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour so that profit-driven criminals may move to other forms of illegal conduct.*
- *The COVID-19 pandemic is also impacting government and private sectors' abilities to implement anti-money laundering and counter terrorist financing (AML/CFT) obligations from supervision, regulation and policy reform to suspicious transaction reporting and international cooperation…"*

Despite these warnings, fraudsters will continue to exploit any opportunity brought about by government policy changes relating to the COVID-19 pandemic.



GOVERNMENT SUPPORT PROGRAMME FRAUDS

As mentioned before, the government launched several support programmes to mitigate the economic impact of the COVID-19 pandemic.

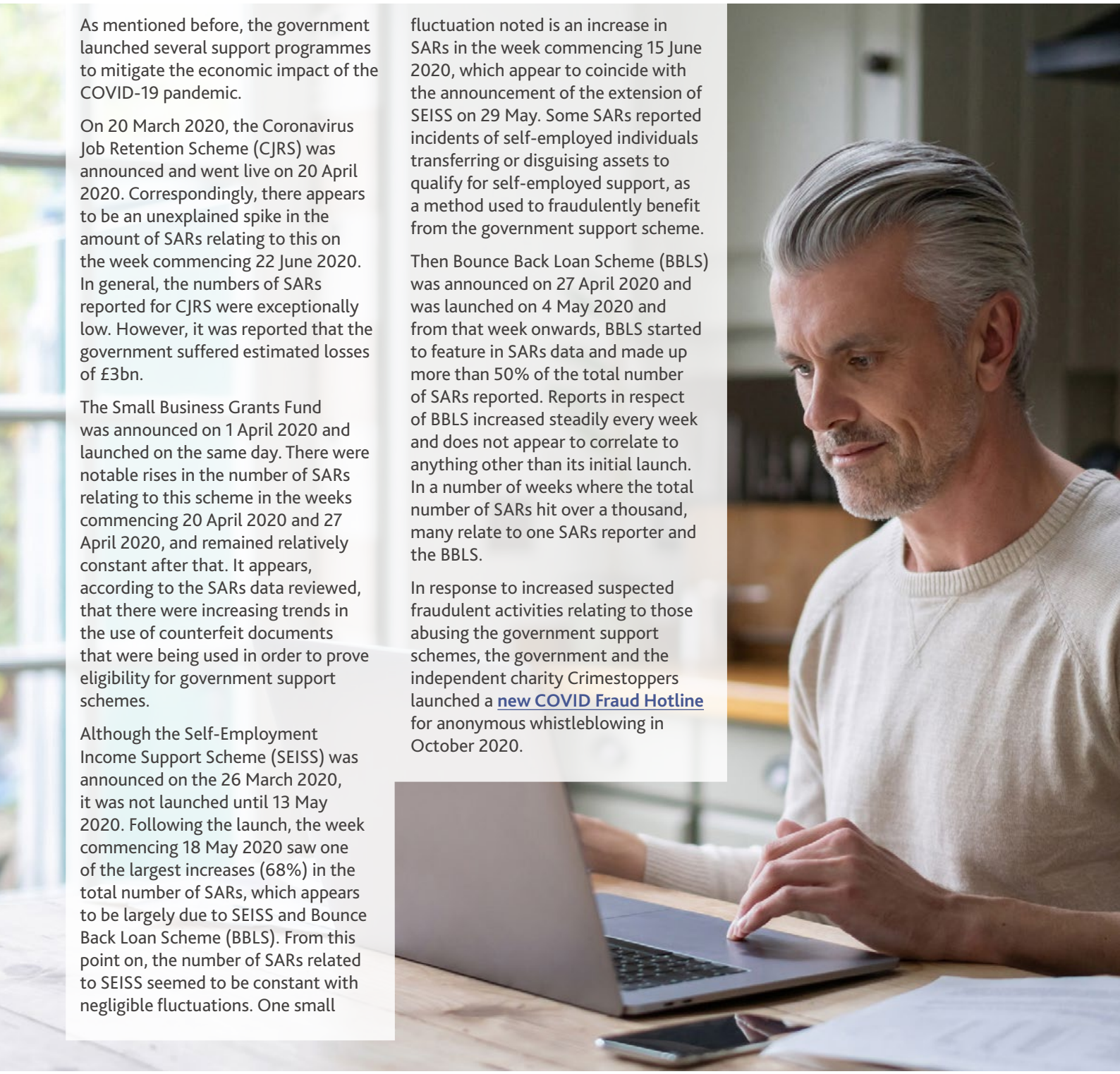
On 20 March 2020, the Coronavirus Job Retention Scheme (CJRS) was announced and went live on 20 April 2020. Correspondingly, there appears to be an unexplained spike in the amount of SARs relating to this on the week commencing 22 June 2020. In general, the numbers of SARs reported for CJRS were exceptionally low. However, it was reported that the government suffered estimated losses of £3bn.

The Small Business Grants Fund was announced on 1 April 2020 and launched on the same day. There were notable rises in the number of SARs relating to this scheme in the weeks commencing 20 April 2020 and 27 April 2020, and remained relatively constant after that. It appears, according to the SARs data reviewed, that there were increasing trends in the use of counterfeit documents that were being used in order to prove eligibility for government support schemes.

Although the Self-Employment Income Support Scheme (SEISS) was announced on the 26 March 2020, it was not launched until 13 May 2020. Following the launch, the week commencing 18 May 2020 saw one of the largest increases (68%) in the total number of SARs, which appears to be largely due to SEISS and Bounce Back Loan Scheme (BBLS). From this point on, the number of SARs related to SEISS seemed to be constant with negligible fluctuations. One small fluctuation noted is an increase in SARs in the week commencing 15 June 2020, which appear to coincide with the announcement of the extension of SEISS on 29 May. Some SARs reported incidents of self-employed individuals transferring or disguising assets to qualify for self-employed support, as a method used to fraudulently benefit from the government support scheme.

Then Bounce Back Loan Scheme (BBLS) was announced on 27 April 2020 and was launched on 4 May 2020 and from that week onwards, BBLS started to feature in SARs data and made up more than 50% of the total number of SARs reported. Reports in respect of BBLS increased steadily every week and does not appear to correlate to anything other than its initial launch. In a number of weeks where the total number of SARs hit over a thousand, many relate to one SARs reporter and the BBLS.

In response to increased suspected fraudulent activities relating to those abusing the government support schemes, the government and the independent charity Crimestoppers launched a **new COVID Fraud Hotline** for anonymous whistleblowing in October 2020.



INVESTMENT FRAUDS, PRIVATE SECTOR FRAUDS AND FRAUDS RELATING TO INDIVIDUALS

At the start of the pandemic, there were widespread reports of private sector frauds and scams against individuals. This appeared to be because fraudsters were taking advantage of the confusion the pandemic brought. Examples included an investment fraud in the form of a hoax scheme purporting investment into a vaccine production business, refunds being claimed from fake holiday bookings and romance fraud. These were all recorded in the SARs data for the week commencing 23 March, the beginning of the first UK lockdown.

Early in November 2020, Action Fraud also revealed it had received 17,000 reports of investment fraud totalling £657.4m in the past 12 months, which represents a 28% increase on the year before. There has been a particular uptick in investment frauds.

Some of the cases reported in SARs, included instances where websites or credentials of legitimate investment managers and Independent Financial Advisers had been mimicked and individuals and institutions were being offered the opportunity to invest in companies selling PPE and hand sanitiser or working on virus vaccines. There was also the case of a professional services firm that had been approached by individuals wishing to set up an investment fund and requiring professional advice. As it turned out, none of these individuals had any credentials in the field, which suggested to the SARs reporter that these individuals were potential fraudsters who wanted to use the name of their firm to provide credibility.

As recent as January 2021 warnings were issued by a **US drug company** for people to be wary of investment scams using its name to offer the coronavirus vaccine in exchange for money. Also, in January 2021, there were reports of a fraudster who claimed to work for the NHS that injected a 92 year-old woman with a fake COVID-19 vaccine after being charged £160.

Again, it can be seen that fraudster are exploiting opportunities presented by the COVID-19 pandemic and that they may have used the government's COVID-19 policies to coordinate and time their actions.

IS THERE A CORRELATION BETWEEN THE UK GOVERNMENT'S COVID-19 POLICIES AND FRAUD TYPOLOGIES?

The correlation between some of the government COVID-19 policies and the emergence and increase of specific fraud typologies reported in SARs is apparent. These observations though not novel, are evidential and seems to be a reasonable inference that they may be linked.

Many of the frauds highlighted in this article are not new and some businesses are alert to the risks. However, the changes to the ways of working and business operating environment have provided fraudsters with opportunities to exploit. Accordingly, it is observed that there has been an increase in successful frauds and reports of potential frauds triggered by the policy changes announced by the government due to the COVID-19 pandemic. The lockdowns and other restrictions have had organisations and individuals moving their operations predominantly online or over the telephone, providing many and varied ongoing opportunities for fraudsters

Crucially, these observations also demonstrate is that it may be possible for businesses to forecast or predict fraudsters' behaviours or at the very least identify particular areas of their operations that are likely to be targeted, allowing them to mitigate these fraud risks by being proactive.

Conversely, inadequate fraud risk management, a lack of preparation and an absence of defence strategies all increase the risk of becoming a victim of fraud. Accordingly, understanding fraudsters' behaviours could help organisations target their resources for fraud risk management and response plans more effectively. Such understanding is all the more important when businesses are under pressure to cut costs

PREVENTION IS TYPICALLY BETTER THAN CURE

The occurrence of the COVID-19 pandemic has seen exponential growth in and resurgence of various fraud typologies, and the emergence of 'new' fraudulent activities especially in the area of cybercrime. To protect themselves, organisations should invest in fraud prevention and preparedness strategies.

With no fraud detection lexicon to default to and no previous fraud experience, some organisations have developed the mind-set and an organisational culture of 'it-won't-happen-to us'. Short-sighted ways of thinking such as this, increase an organisation's vulnerability and make it an easy target for fraudsters, both internal and external. Being proactive will counter or at the very least help minimise organisations' vulnerabilities. Data included at page 5 of the ACFE 2020 Global Study on Occupational Fraud and Abuse shows that the use of targeted anti-fraud controls is associated with lower fraud losses and quicker detection.

Matching an organisation's fraud prevention objectives with fraud awareness are crucial in the fight to mitigate and deter fraud. Organisations, therefore, should create a culture that focuses on fraud prevention and deterrence, and staff should be educated on the possible ramifications of fraud. It is especially important that fraud prevention plans are dynamic so as to keep up with or have an objective to keep ahead of fraudsters' strategies and tactics.

KEY TAKEAWAYS

Organisations are at a higher risk of experiencing fraud during the COVID-19 pandemic but paying close attention to their environment and the events that fraudsters may exploit can help to mitigate these fraud risks. Building and strengthening fraud resilience is essential, especially during the COVID-19 pandemic. Organisational fraud prevention and deterrence strategies should consider a 'just-in-case' proactive approach as an essential component in helping to protect against potentially catastrophic consequences. Accordingly, organisations need to assess their anti-fraud policy and if they do not have one, put one in place to ensure that they do whatever it takes to build a resilient organisation, which is proactive in their approach to combatting fraud.

Organisations should therefore:

- Set organisational tone from the top down that makes clear that fraud prevention and detection plans are in operation
- Pay closer attention to the internal and external environment in which their businesses operate and tailor fraud prevention plans as required
- Undertake regular fraud risk assessments in response to the frequent evolution of fraud
- Act to mitigate any perceived or identified fraud risk
- Consult with or engage fraud practitioners at the outset of drafting and implementing risk management and fraud prevention strategies
- Speak to fraud practitioners as soon as possible to assist with possible recovery and minimise further losses, if they become fraud victims.

Frauds are one of the biggest threats to organisations. Without the right fraud prevention and detection measures, they are at risk of great reputational and financial damage. Although the government has recently announced the possible lifting (subject to certain conditions) of all legal limits on social contact by 21 June 2021, the effects of the COVID-19 pandemic on fraud and the government's response will be felt for some time to come.

Fraudsters will be planning their next move, determining who the soft targets are, the method and the depth of their schemes. In response, organisations must act now more than ever to ensure they are one step ahead. If you would like advice on how to assess fraud risks and how to make effective investments in fraud prevention, please get in touch.

Want to further explore recent fraud trends affecting all companies? Read our FraudTrack 2021 research. FraudTrack, an annual report compiled by BDO since 2003, tracks reported fraud cases valued at over £50,000 in the UK from December 2019 to November 2020. Each year we analyse the nature of reported fraud from a variety of open news and reporting sources. We have witnessed and studied the rise of fraud from £331 million to over £2 billion in recent years.

FOR MORE INFORMATION:

KAREN EDWARDS
SENIOR MANAGER,
FORENSIC ACCOUNTING

+44 (0)20 3219 4871
karen.edwards@bdo.co.uk

KALEY CROSSTHWAITE
PARTNER,
HEAD OF FORENSIC ACCOUNTING
AND VALUATION SERVICES

+44 (0)20 7893 3548
kaley.crossthwaite@bdo.co.uk

www.bdo.co.uk

21-04-2394