HERBERT SMITH FREEHILLS

PRESSURE POINTS: COVID-19 AND FRAUD (UK)

10 July 2020 | UK
Legal Briefings

Covid-19 restrictions are being slowly eased, but the impact of the pandemic and related lockdown measures on financial crime risk and on related compliance measures continues to be a high priority for business. In our April briefing, we analysed the impact of the restrictions on the UK criminal justice system – in particular, the practical issues facing law enforcement agencies (**LEAs**), the courts and the prison service.

Even before the pandemic, fraud was the single most common crime in the UK, accounting for approximately one-third of all crimes. The estimated annual cost to the UK is an estimated £190bn, the majority of which (£140bn) is borne by the private sector (and that is to ignore the impact of the estimated 80% of all fraud that goes unreported[1]). In this briefing, we take a look at the fraud risks arising as a result of the pandemic and the measures being taken in response, including:

- the UK Government's economic and employment schemes;
- the impersonation of officials;
- medical supplies;
- consumer fraud;
- cyber-enabled fraud; and
- volunteering and charity fraud.

We also briefly consider the response of LEAs to these developments, and provide links to other useful materials and guidance.

In addition, we discussed Covid-19 related financial crime risks and relevant risk mitigation measures in the first episode of our Corporate Crime and Investigations annual London conference webinar series, and clients who would like to listen to a recording of the webinar (or attend the rest of the series) can register here.

Government Schemes

The UK Government has introduced a number of schemes designed to protect businesses and individuals from the economic impact of the Covid-19 restrictions. Its flagship policy is the Coronavirus Job Retention Scheme (**CJRS**), under which the Government contributes 80% towards a furloughed employee's wages. There are also schemes relating to Government-backed loans, claiming back sick pay, deferral of income tax and VAT payments, and business rates relief.

The Government accepted, when it rolled out the schemes, that they carried an inherently high risk of fraud; primarily posed by applicants either misrepresenting their situation or impersonating eligible individuals or businesses, in order to qualify.

Recent statistics demonstrate that these risks have, in fact, played out. Her Majesty's Revenue & Customs (**HMRC**) has announced that it has received 1,868 reports relating to fraudulent use of the CJRS to the end of May 2020. Whistleblowing charities say that they have received thousands of reports of furloughed employees being asked to continue working, which is not allowed under the rules of the scheme.

The Government has created a Covid-19 Counter Fraud Response Team to help public bodies in minimising these risks. Its advice focuses on "*frictionless up front checks*" and "*post event assurance*", as well as the use of data analytics, in order not to delay urgent payments and services.[2] The advice accords with the FCA's "Dear CEO letter" which allowed for flexibility for firms in complying with their client identity verification obligations (as discussed in an earlier post).

The emphasis on implementing the schemes quickly suggests that there will be widespread after-the-event investigations, out of which prosecutions for fraud, theft or false accounting seem likely – especially if Covid-19 offences remain an "*immediate priority*" under the Interim Charging Protocol issued by the Crown Prosecution Service and National Police Chiefs' Council. There is also the possibility that fraudulent CJRS claims might lead to the first prosecutions for the failure to prevent tax evasion offence under the Criminal Finances Act 2017.

Businesses utilising the CJRS or other government schemes will wish to be able to show HMRC that reasonable prevention procedures were followed, in the event of an investigation. In practice, it will be helpful for businesses to:

- demonstrate that procedures are actively monitored;
- review risk assessment and re-evaluate controls, taking account of new risks and processes; and
- communicate changes to procedures to prevent facilitation and reinforce existing procedures with training.

Businesses dealing with companies which are utilising the government schemes should be alert to red flags, and some businesses (such as financial institutions or accountants) may be particularly well placed to observe and report suspicious activity. There have been a number of updates made publicly available by the National Crime Agency (**NCA**) and other bodies to date which flag the following:

- funds claimed by businesses utilising government schemes being withdrawn quickly, either as cash or transferred to a third party, suggesting possible 'mule' activity;
- companies using CRJS funds to pay the salaries of employees who continue to work;
- claims under the self-employment income support scheme where there is a lack of evidence of self-employment (or positive evidence of salaried employment); or
- claims for bounce-back loans by businesses which show minimal activity prior to the receipt of the loan, fund transfers to personal accounts or third parties, rapid cash withdrawals, or multiple loan applications using different business names.

Specifically in the context of providing bounce-back loans, the FCA has also issued guidance on customer due diligence obligations in respect of new and existing customers (which fits within the framework of its prior "Dear CEO letter", discussed in our earlier post, and later update on financial crime systems and controls during coronavirus, both of which emphasise the need to continue to comply with core client identity verification obligations – but the scope for flexibility in doing so).

Impersonation of Officials

Criminals are also targeting the public off the back of government schemes. The Financial Action Task Force (**FATF**) has identified impersonation of government officials as an increased fraud risk, as a result of the increase in government grants and tax relief schemes.[3] For example, there has been a sharp rise in phishing emails purporting to be from HMRC requesting bank details in order to make a claim through the CJRS. Interpol has also reported criminals impersonating hospital officials claiming they require payment to treat sick relatives.

Businesses will need to consider what training or awareness-raising for staff and, in respect of some businesses, for customers, will be appropriate to seek to mitigate these threats.

Medical Supplies

The sudden spike in demand for personal protective equipment (**PPE**), sanitiser and testing kits is a further concern. Europol has identified the sale of counterfeit medical goods as one of its four main areas of risk; approximately 34,000 counterfeit surgical masks were seized by LEAs worldwide in one week in March. Europol is also investigating a €6.6m fraud relating to the non-delivery of face masks and alcohol gel.[4]

In the UK it is perhaps too soon to expect there to have been many reported investigations or prosecutions, but the UK's Medicines and Healthcare products Regulatory Agency has said it is investigating 14 instances of the sale of "FakeMeds" and the NCA has reported two instances of arresting individuals for selling fake tests.

The UK Financial Intelligence Unit (**UKFIU**), which processes suspicious activity reports (**SARs**) has noted the increase of cases involving the supply of PPE, both in relation to large-scale procurement contracts and online sales to the public. Three main forms of criminality appear to be emerging:

- as discussed above, there appear to be significant volumes of fraudulent sales, where either the products do not arrive or counterfeit goods are delivered. FinCEN, the US FIU, has issued helpful guidance (albeit with a somewhat US flavour) on red flags relating to this type of activity, available here;

- the urgent need to obtain large volumes of PPE has led some governments (and businesses) to procure goods outside normal procurement frameworks. Where significant funds are expended and normal due diligence and tender requirements are side-stepped, there is an obvious risk of funds being diverted corruptly. Our Johannesburg office commented on this risk area in this recent article on 'Covid-capture'; and

- it also appears that non-existent Government procurement contracts are being used to support transfers of money[5], i.e. purported trade in PPE is being used to mask the laundering of funds obtained from other forms of criminality.

Whilst SARs only evidence suspicions of money laundering, the increase does suggest that fears around medical-related fraud have borne out, and close attention will need to be paid to PPE-related opportunities and transactions on an ongoing basis.

Fraud Targeted at Consumers

The FCA has identified a number of scams targeting individuals who face financial worries, as a result of the economic impact of the restrictions, including:

- "loan fee fraud", where scammers ask for an upfront loan fee (often between £25 and £450) without providing credit;
- "good cause" scams, where investment is sought for the production of PPE, sanitiser or new medicines; and
- "clone firms" imitating authorised firms seeking to sell, promote or advice on sale of insurance products, as well as relating to pension advice and investments.

FATF has identified similar concerns, highlighting, in particular, microcap stocks, typically issued by the smallest companies, as being vulnerable to fraudulent investment schemes, as they are low-priced with often limited publicly available information.

In an example of a cross-over between two of the risk areas mentioned above, in the US, the head of a medical technology firm, Arrayit Corp, and an investor have been charged in connection with schemes to defraud the US Medicare programme and mislead investors over Covid-19 tests. The US Securities and Exchange Commission has commenced a separate civil action under which an individual trader is alleged to have posted false statements online in an effort to drive up the price of Arrayit shares and subsequently sell them (a "pump and dump" scheme). The trader is also alleged to have engaged in "spoofing" (a practice by which the appearance of demand for a stock is artificially created).

Action Fraud reported, as at 12 June 2020, 2,378 Britons have been defrauded at a cost of £7.1m due to Covid-19 related scams, with 12,323 reports of Covid-19 related phishing emails having been received. In addition, the FCA's register was cloned in June 2020 and a fake register published online, presumably in the hope of making it more difficult for consumers to spot fraudulent firms.

Action Fraud's webpage contains useful anti-fraud tips and guidance for consumers. There are also some indications that scams against individuals have decreased since the early phase of the pandemic, with fewer such SARs being made.

Cyber-Enabled Fraud

Much of the fraudulent activity described above is cyber-enabled, and businesses have also been subject to an uptick in phishing, CEO-fraud and related scams. As detailed in our cyber security team's recent blog, the UK National Cyber Security Centre and US Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency have issued a rare joint advisory detailing practical advice for individuals and organisations on how to deal with Covid-19 related malicious cyber activity, which provides some practical advice that individuals and organisations can follow to reduce the risk of being affected by malicious cyber actors. The team's earlier podcast discusses some of the cyber security risks that have been made more acute by the current disruption, including fraud and ransomware attacks, and the steps needed to deliver cyber and data security operational resilience.

Volunteering and Charity Fundraisings

In addition to the more complex crimes reflected above, the National Trading Standards (**NTS**) has reported instances of criminals targeting older people with offers to do their shopping, taking money for the purchases and failing to return. Similarly, criminals have been making fraudulent claims that they are collecting donations for Covid-19 related causes, such as collections for key workers.[6]

LEAs' Response

Covid-19 related offences, including fraud and dishonesty offences against vulnerable victims, are presently designated as "*immediate priority*" cases under the Interim Charging Protocol (discussed in our previous briefing). The Serious Fraud Office (**SFO**), the Financial Conduct Authority (**FCA**) and the NCA have all publicly committed to holding to account anyone who seeks to take advantage of the current situation.

However, there are concerns about the justice system's ability to do so; jury trials have stalled and the backlog of cases continues to grow. The SFO, in particular, has long faced criticism for the delay in its investigations and it recently confirmed that it has stopped conducting compelled interviews. It has, however, accepted recommendations by Her Majesty's Crown Prosecution Inspectorate relating to its resourcing – we wait to see what impact this will have on the expedition of its cases.

The Interim Charging Protocol also categorises non-Covid-19 serious fraud as lower priority, which means that efforts to combat specific Covid-19 frauds are likely to come at the expense of tackling the wider prevalence of fraud in the UK.

In light of these difficulties, it seems likely that many cases will either not be investigated or will be dealt with outside the criminal system. For example, the Government has proposed revisions to the Finance Bill 2020 that will make it easier to recover CJRS payments that were inappropriately claimed or used, and to impose civil (financial) penalties where the inappropriate claim/use was "*deliberate*".[7] The proposed amendments will make it easier to deal with tax fraud, such as making company officers jointly and severally liable where they have deliberately claimed for CJRS assistance. If these revisions are enacted, it is likely that prosecutions (which are more onerous for LEAs than civil enforcement processions) would be reserved for only the most serious instances of CJRS abuse.

Conclusion

LEAs worldwide have identified broadly similar fraud risks arising out of the impact of Covid-19, the related restrictions and new working practices. In particular, the UK Government's economic and employment schemes were rolled out with speed and an acceptance that they were inherently risky. Similarly, the increased demand for PPE, testing kits and other medical equipment provides opportunities for fraudsters.

Many businesses and individuals are financially vulnerable, putting them at an increased risk of fraud schemes, some of which are discussed in this briefing. On the other side of the equation, the economic downturn will likely motivate some individuals to commit economic crimes, including fraud, false accounting, tax evasion and insider dealing, and bring to light pre-existing criminality as businesses experience financial difficulty.

LEAs have issued tough statements on enforcement action and the designation of Covid-19 related fraud as an immediate priority does show that this is a prime concern for prosecutors. However, there are many practical obstacles to effective enforcement – particularly, stretched resources and congestion in the courts' case lists. In the meantime, businesses will need to review their financial crime risk assessments and keep their policies and procedures up to date, as the fraud landscape continues to shift.

Endnote: further information regarding Covid-19 fraud risks can be found at the following links to publications from Government, LEAs and watchdogs.

More on Catalyst //

---

[1] NCA: Fraud Hub

[2] UK Government Counter Fraud Function: Fraud Control in Emergency Management: Covid-19 UK Government Guidance

[3] FATF: Covid-19-related Money Laundering and Terrorist Financing Risks and Policy Responses

[4] Europol: How criminals profit from the Covid-19 pandemic

[5] UKFIU: Covid-19 SAR – 29 May 2020, Issue 2

[6] NTS: Beware of Covid-19 scams

[7] HMRC: Corporation Tax / Income Tax – Taxation of Coronavirus Support Payments

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

SUSANNAH COGMAN
PARTNER, LONDON

+44 20 7466 2580
Susannah.Cogman@hsf.com

PHOEBE JERVIS
ASSOCIATE, LONDON

+44 20 7466 2805
phoebe.jervis@hsf.com

BRIAN SPIRO
PARTNER, LONDON

+44 20 7466 2381
brian.spiro@hsf.com

KATE MEAKIN
PARTNER, LONDON

+44 20 7466 2169
Kate.meakin@hsf.com

DANIEL HUDSON
PARTNER, LONDON

+44 20 7466 2470
Daniel.Hudson@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2021

SUBSCRIBE TO STAY UP-TO-DATE WITH LATEST THINKING, BLOGS, EVENTS, AND MORE
Close

© HERBERT SMITH FREEHILLS LLP 2021