CORONA CRIME

With plans across the world to gradually lift some lockdown restrictions we can expect to uncover a new wave of corporate criminal activity and organised crime at home and abroad. Criminal defence specialists Simon Pentol QC and Duncan Jones of 25 Bedford Row examine the likely trends and the focus of investigation by the authorities.

Prosecutorial response to lockdown

COVID-19 and the lockdown have created an unprecedented crisis in the criminal justice system, causing a huge hiatus in both the trial process and the investigative process.

The Crown Prosecution Service has been forced to review large numbers of prosecutions and consider carefully what cases are to be charged and fed into courts at much reduced capacity. However, the CPS COVID-19 crisis response and Interim CPS Charging Protocol published on 30 March 2020 states that all COVID-19-related cases, including dishonesty against vulnerable victims and COVID-19 related fraud are an "immediate" priority.

Although the Serious Fraud Office has been affected by lock-down and remote working necessary for social distancing, it issued a statement on 7 May 2020 that it has been "able to continue to follow active lines of inquiry in open investigations, as well as looking into allegations and referrals at the "pre-investigation" stage. That has not included any searches or interviews since lockdown began. The SFO nevertheless said that "*Fraudsters will look to use the uncertainty of the coronavirus crisis to scam innocent people out of their money. The SFO is united with its law enforcement partners in our desire to prevent such fraud and hold the perpetrators to account."* A small sign that its 'business as usual' will be taken from the resumption, after a lengthy adjournment, of the SFO prosecution of Unaoil and SBM executives accused of corruption at the Old Bailey, having transferred from Southwark Crown Court to enable social distancing.

The Financial Conduct Authority has been equally bullish within its published guidelines aimed at instructing businesses and protecting consumers whilst ensuring that fraud continues to remain an enforcement priority.

The National Crime Agency has echoed its commitment to work alongside its regulatory partners to militate against fraud and prosecute criminals seeking to take advantage of the current crisis.

By contrast, HMRC has taken a more pragmatic approach by using a compliance strategy and focusing now on reaching financial settlements under its civil enforcement COP9 regime.

New trends in crime

Criminals have been quick to seize upon new opportunities to engage in criminal activities that arise from national governments across Europe seeking to safeguard public and economic safety by taking measures in response to the COVID-19 pandemic.

Measures introduced across Europe have led to:

- An unprecedented demand for certain goods, PPE & pharmaceutical products, with counterfeit and non-existent goods sold to public and private victims;
- Decreased mobility and flow of people and goods across Europe;
- An unprecedented number of citizens staying at home with an exponential increase in use & reliance upon digital communication and teleworking;
- The effect of lockdown forcing criminal activity indoors via online crime;
- Increased anxiety being caused to populations resulting in vulnerability to exploitation;
- Decreased supply of certain illicit goods (guns & drugs) in and from Europe; and
- Abuse of government financial schemes (Furlough and tax/business relief).

Public Sector Fraud

In guidance published on 26 March 2020 for leaders and fraud experts in government bodies and local authorities administering emergency programmes, the government acknowledges that fraudsters will try to take advantage of measures designed to mitigate the economic effects of lockdown. The guidance suggests that Public bodies can *"reduce the threat of widespread fraud by integrating low-friction controls into payments where possible, and carrying out post-event assurance work."*

The guidance describes two imminent threats to the public sector:

1. First party application fraud – the risk that an application may misrepresent their circumstances to qualify for a government grant or scheme;
2. Third party impersonation fraud – the risk that a third party may impersonate a business to extract grant funding from the government.

Although speed has been of the essence in distributing aid, there is no doubt that audits and investigations will follow once the health crisis subsides. The guidance refers to a COVID-19 Fraud Response Team and recommends *"a post-event assurance process to ensure funding is used for its intended purpose"* including sample-checking high-risk grants for fraud, invoking claw-back arrangements and pursuing recovery.

Benefit and revenue fraud

The head of the UK National Crime Agency, Lynne Owens, warned last week that Corona Virus relief schemes were targets for fraud against the Department for Work and Pensions and HM Revenue and Customs. She said that law-enforcement officials were aware that organised criminals would seek to exploit furlough and business relief schemes for profit and recognised that risk can be created by a new stimulus package. The BBC reported that benefit officials fear that as much as £1.5bn may have been lost to fraudulent claims for Universal Credit during the pandemic and the cost of other forms of financial crime will be far greater.

Phishing and impersonation

In the first month of lockdown, individual cases of fraud valued at circa £800,000 directly related to Corona Virus were recorded by Action Fraud alone. Many are phishing scams attempting to trick people into opening malicious attachments or revealing sensitive personal

and financial information. One such fraud involves contacting potential victims by email, purporting to be from research organisation's affiliated with the Centers for Disease Control and Prevention (CDC) and the World Health Organisation (WHO). The fraudsters claim to be able to provide the recipient with a list of coronavirus infected people in their area and the victim is asked to click on a link that leads to a malicious website, or is asked to make a payment in Bitcoin. There are many other reported examples of fake government grant phone calls and text messages offering tax rebates with links to websites impersonating HMRC designed to harvest bank details.

Accounting fraud

The UK Government response to the threat of Coronavirus has resulted in unprecedented restrictions on the normal economic activities of businesses and individuals. The lockdown restrictions caused immediate and dramatic reductions in cash flow for many businesses, with many struggling to survive. At a time of exceptional pressure, every penny counts and losses become difficult to disguise. As the tide goes out in times of economic downturn – in this instance a severe and immediate recession followed by a likely depression – experience shows that corporate and financial crimes are often left on the beach. Creative or unlawful accounting or debt structuring that may be quick to turn over in times of growth will inevitably be uncovered as credit becomes harder to access. Investors seeking to withdraw from investment schemes that once seemed attractive, may discover that they can no longer access funds.

Furlough Fraud:

An obvious target for abuse lies within the Coronavirus Job Retention Scheme (the 'furlough scheme') that was launched by the UK government on 20 April 2020 to remain in force until October 2020 in order to reimburse businesses for up to 80% of the wages of staff (capped at £2,500 per month) forced to take a leave of absence but otherwise kept on the payroll throughout lockdown. Through force of circumstance the scheme had to be organised quickly and sources predict it could cost circa £40 billion over three months if as many as 8 million people are furloughed at an 80% subsidy. Although the Treasury has issued guidance, HMRC acknowledge the potential for fraudulent claims by stating that these will likely result in criminal convictions. Moreover and significantly, HMRC has stipulated that businesses that seek furlough compensation need to keep their records for five years – a clear hint that retrospective audits will be undertaken.

Given that HMRC investigations are often heavy-handed and premised upon the 'guilty unless proven innocent' doctrine, it is imperative that organisations that take advantage of the scheme do so by adhering to the rules and maintain their records accurately in the event of likely retrospective investigation.

Eligibility for furlough leave is that employees do not work – the rules stipulate that employees "cannot undertake work for, or on behalf, of the organisation or any linked or associated organisation. This includes providing services or generating revenue." This is not clear-cut and can create genuine difficulties for staff and organisations alike:

- What if a furloughed employee is put under pressure to go back to work as a 'volunteer' and told that it is permissible for he/she to do so?
- What of staff who work on commission that itself falls outside the scheme?
- The Treasury encourages furloughed staff to visit the 'Report Fraud to HMRC' page of the online portal. But in the current climate of economic uncertainty, what are whistleblowers realistically expected to do in the event they believe or uncover a fraud being committed by their employer - especially if threatened with redundancy and loss of income?
- The guidance makes clear that furloughed staff should be encouraged to undertake training. But where does working on behalf of a business end and training begin? And In which case, shouldn't those staff members be paid national minimum wage or otherwise have their wages topped up?
- And what of furloughed company directors? The guidance suggests that activities amounting to their duties under the Companies Act 2006 are permitted but where do filing of accounts end and the preparation of business records that generate business revenue, begin?
- More complicated is the issue of TUPE [Transfer of Undertaking (Protection of Employment) Regulations 2006] concerning the protection of employees' rights when the organisation for which they work transfer to a new employer. For those not on the payroll of their new employer on the scheme's cut-off date of 28 February 2020, are they eligible or not for furlough compensation if claimed by their new employer?

The scope for potential theft and fraud offences under the Job Retention Scheme appears wide and will include:

- Employer benefit fraud – whereby a business reduces its payroll by taking advantage of the scheme but nonetheless instructs its staff to work;
- Employee benefit fraud – whereby a business generates furlough income on behalf of employees not genuinely employed by it; and
- False accounting or fraud by misrepresentation in respect of false or improper furlough claims being based on inaccurate information.

To avoid prosecution or to properly defend itself in the event of current or retrospective investigation, it is imperative that businesses seeking furlough relief have in place and maintain a protocol demonstrative of:

- Proper payroll training and understanding of the eligibility requirements;
- Maintaining on-going checks to ensure no furloughed staff member is working (as defined);
- Maintaining compliance policies;
- Answering queries raised by employees;
- An audit trail with HMRC; and
- Taking expert legal advice.

International and Organised Crime

On 27 March 2020 Europol published a situational report across four main areas of crime as follows:

1. **Cybercrime:** Use of malware packages as greater number of employers institute telework and allow connections to their organisations' systems. For example, the Czech Republic reported a cyber attack on Brno University Hospital that resulted in it shutting down its IT network;

2. **Fraud:** Europol is investigating the transfer of €6.6m to a company in Singapore for non-existent alcohol gels & FFP3/2 masks;

3. **Organised Property Crime:** There is a likely increase in scams involving the impersonation of representatives of public authorities and the targeting of commercial premises & medical facilities for organised burglaries. This poses a dynamic threat during the crisis and its aftermath. Multiple EU member states report access to private homes by criminals impersonating medical staff conducting a "Corona Test."

4. **Counterfeit & Substandard Goods**: Sale of counterfeit healthcare, sanitary products, PPE & counterfeit pharmaceutical products has increased manifold since the outbreak of the crisis. This creates the obvious risk that counterfeiters will fill shortages in the supply chain by providing counterfeit alternatives both on and offline. 34,000 counterfeit surgical masks were seized by law enforcement agencies worldwide as part of Operation Pangea supported by Europol.

Trafficking drugs under the cover of Corona Virus

The NCA reports significant border seizures during lockdown including a quarter of a tonne of cocaine on 05 May 2020 secreted under medical dry ice that was falsely addressed to a hospital in London.

A new report entitled 'County Lines after Covid' by Crest Advisory claims that County Lines drug dealers have moved their operations by recruiting youngsters from small towns rather than big cities to avoid attracting attention during lockdown. "Cuckooing" (gang members taking over the home of a vulnerable person for use as a drugs den) has been replaced by "stacking" whereby gangs send text messages to their customers to be at a designated place at a designated time whereupon a dealer will arrive and complete a large number of deals.

It will take years to count the vast human and economic cost of COVID-19, but an important part of the recovery will be the investigation and prosecution of financial crime and organised crime. This will present fresh challenges to investigators and defenders alike.

Simon Pentol QC
Duncan Jones
25 Bedford Row