FINANCIAL CRIME NEWSLETTER

CROSSED WIRES

Written by Richard Whittam QC

A year ago Lisa Osofsky, the Director of the Serious Fraud Office (SFO), in an interview with the Evening Standard, said that she planned to work with HM Revenue and Customs to uncover breaches and then tell offenders: '*You can spend 20 years in jail for what you did or wear a wire and work with us"* (Evening Standard, 26 April 2019).

It was a statement that attracted attention, with commentators interpreting it as going far beyond revenue prosecutions and debating the practical application of such a bold announcement in relation to the principal statutes that govern how the State should conduct such investigations. The Regulation of Investigatory Powers Act 2000 governs the use of covert human intelligent sources. The framework for immunity from prosecution or a reduction in sentence is set out in The Serious Organised Crime and Police Act 2005 (SOCPA), albeit the common law system of credit for co-operation was not expressly abolished.

It was not a novel suggestion. In her keynote address at the 35th Foreign Corrupt Practices Act Conference in Washington DC on 28 November 2018 Ms Osofsky said:

> *"We are going to learn best practices and use tools effectively pioneered elsewhere. For example, we in the UK have heard loud and clear from our colleagues in the United States how valuable co-operators can be in cracking white collar cases. We have different practices and different rules in Britain, and co-operators have, to date, been more widely used in narcotics or gang cases. Suffice to say, we are intently exploring this area in the white collar world."*

In her oral evidence before the Justice Committee of the House of Commons on 18 December 2018 she said:

> *"The other side of what I have been doing is a little more external. I have spent an awful lot of time working with, often, the Americans, because we have a lot of cases going with them. There are so many avenues for co-operation there, including shared use of important intelligence information that, especially in a white-collar case, can really crack open our cases. It helps us work at pace if we can get an insider who can help us understand what the scheme was and what the relevant documents are, and then, when we come to trial, we have someone there to bring it to life. We do not just have a case where the jury looks at mountains of documents and does not have a live witness at the centre."*

Well before Ms Osofsky took over in August 2018, the SFO's then General Counsel, Alun Milford, spoke of the SFO's use of information to discern and control risk at the Cambridge Symposium on Economic Crime 2014. He said of suspects and/or defendants:

> *"Some are contrite and, having found themselves embroiled in events they had not planned or in a toxic corporate culture, might simply want now to do the right thing. Others have more practical considerations and decide to help us because they calculate it is advantageous to them to do so. Unsurprisingly, I think they are right. By their very nature our cases involve serious offending of a kind that can attract severe sentences. Sentencing is a matter entirely for the judiciary, and so prosecutors are in no position to make assurances about outcomes. However, the courts have made clear that co-operation of the kind envisaged in SOCPA, particularly sections 73 and 74, concerning a defendant's supply of information both to the SFO and to a jury, can make a real difference in sentence."*

A year on from Ms Osofsky's statement, little appears to have changed. Whilst the SFO has enjoyed some successes, there have been notable failures, particularly in the prosecution of individuals after the corporate

body had accepted there had been behaviour that warranted a Deferred Prosecution Agreement (DPA). In July 2016 Sarclad Ltd entered into a DPA, but three years later, in July 2019, the three individuals prosecuted were acquitted. In October 2019, Güralp Systems Ltd entered into a DPA, but in December 2019 the three individuals prosecuted were acquitted. Most notably the SFO entered into a DPA with Tesco Stores Limited. The Statement of Facts named three executives who were then to be prosecuted. One was too unwell to face a trial. The trial judge, Sir John Royce, acceded to a submission of no case to answer at the close of the prosecution case. The prosecution unsuccessfully appealed that terminating ruling[1]. The three individuals then applied to Sir Brian Leveson, President of the Queen's Bench Division, to have their names removed from the Statement of Facts. Sir Brian had approved the DPA. He decided that a court that had approved a DPA between the SFO and a company in relation to an overstatement of company profits had no jurisdiction to alter or modify the terms of the agreement in order to reflect the acquittal in parallel criminal proceedings of three of the company's former employees whose alleged wrongdoing was detailed in the agreement. The court's role was limited to enforcing the terms of the agreement.

The failed prosecution of Barclay's Bank plc and four individuals was a double blow for the SFO. An often overlooked observation made by Ms Osofsky in her interview with the Evening Standard is her complaint that the prosecution was '*hamstrung*' by '*antiquated*' laws that hindered the prosecution of corporate offenders. The case against the Bank was stopped by the trial judge, Jay J, but on an application to the Queen's Bench Division for a voluntary bill of indictment, Davis LJ re-affirmed *Tesco v Nattrass* as the route to determining corporate criminal liability[2]. Secondly, not one of the four individuals indicted were convicted.

One argument advanced in relation to the failed prosecutions of individuals is that they were too paper-based. They were circumstantial cases, as often prosecutions of corporate frauds are. As Ms Osofsky had opined, the SFO did not have a witness to bring the case to life: just a jury looking at a mountain of documents and no witness at its centre. That, of course, did not apply to the prosecution of Barclays plc or the individuals in Tesco.

It might be that Ms Osofsky's statement about the use of a wire was somewhat misunderstood, or misplaced. Misunderstood because in the interview with the Evening Standard she had confined her observation to revenue cases, albeit she had no done so in the latter part of 2018 in Washington or before the Select Committee.

Possibly misplaced because usually, although not always, corruption is discovered after the event. Dramatic though it may sound, to have a collaborator '*wired*' during the planning and execution of the conspiracy is unlikely.

Further, poetic license accepted, walking free from a twenty year sentence is improbable. First, it would have to be particularly grievous conduct that would attract such a sentence. Secondly, immunity from prosecution is vanishingly rare.

The use of co-offenders as prosecution witnesses is not altogether straightforward. SOCPA came into force on 1 April 2006. Parliament created a statutory framework which formalised and developed well established common law principles, formerly embraced, in part, in the well understood phrase, "*Queen's Evidence*". There is no requirement for an Assisting Offender (AO) to give evidence; the assistance may be confined to intelligence. The desirability for providing leniency to an AO (whether by way of immunity or reduction in sentence) is a long standing and entirely practical convention.

Section 71 addresses possible immunity from prosecution for an offender who provides assistance in the investigation or prosecution of an offence. Section 72 enables a specified prosecutor to provide an individual with an undertaking that any information provided by him will not be used in evidence. Section 73 governs the arrangements for reductions in sentence in specified circumstances for those who have provided assistance. Section 74 introduces a new process for the review of a sentence which has already been imposed.

As an illustration of the infrequency of use of those provisions, the Crown Prosecution Service's use of immunity under s71 and undertakings as to the use of evidence is rare indeed. In a written answer to parliament on 9 June 2011, the Solicitor General indicated that since 2006 there had been 7 agreements under s.71 and 11 agreements under s.72. In annual correspondence between the DPP and the Attorney

[1] see [2019] EWCA Crim 29
[2] see [2018] EWHC 3055 (QB)

General (the latest being dated 30 October 2019, dealing with events up to 30 April 2019) it is confirmed that since 2011 there have been **no** agreements under s.71.

The first (and considered by many still to be the leading) authority on SOCPA is *R v P; R v Blackburn*, [2008] 2 Cr App R (S) 5. Sir Igor Judge, President of the Queen's Bench Division (as he then was) stated that the Court of Appeal was not considering s.71 or s.72 [§23]. He could not envisage any circumstance in which a defendant would not serve any sentence at all because ss.73 and 74 do not provide immunity from prosecution as s.71 does [§41].

He identified the need for an AO to accept fully their own criminality. That observation has found itself repeated in guidance as to the application of ss.71-74. Whilst those observations are clear and are obviously practical, they are not based on any statutory provision. The real challenge is to have an AO who does not have an axe to grind, or who is not simply attempting to exculpate themselves from a condign sentence.

What happens next? Unless there are current or imminent trials where a witness has been granted immunity from prosecution, Ms Osofsky's observations appear to have been aspirational. Whilst there is a reluctance, at least as far as the CPS are concerned, to enter into an arrangement whereby a witness is given immunity from prosecution, the need for the SFO to have direct evidence of criminality looms large. There is statutory provision for immunity from prosecution, it just needs to be deployed in the appropriate circumstances. The difficulty is identifying individuals who, after the event, will co-operate and who are sufficiently credible to be called as a witness for the prosecution.

REGULATING CRYPTO-CURRENCY – INTERNATIONAL AND NATIONAL TRENDS

Written by Alastair Smith

'*As the value and use of crypto assets have grown, so have the risks for financial crime*'
Director of Retail and Regulatory Investigations, FCA
6th March 2020

Cryptocurrencies have been promoted by some as a "safe haven asset" in these uncertain economic times. The present coronavirus crisis may persuade some individuals and investors to look to the likes of Bitcoin in the hope of gaining sanctuary from market unpredictability or Government intervention. There is a real risk, however, that in trying to avoid a financial storm, investors may walk straight into a regulatory one.

Whilst efforts to define and regulate cryptocurrency trading have been ongoing internationally for several years, there can be little doubt that the pace of regulation worldwide has seen a significant increase over recent months. Despite the ongoing pandemic, many countries have found the time and will to introduce legislation or regulations which directly impact on those who operate in the international cryptocurrency market including:

- On 10th January the European Union's fifth Anti-Money Laundering Directive (5AMLD) came into effect (see below). The Directive envisages a 10th September deadline for Member States to have created central registries.
- On 16th January Canadian lawmakers published '*Staff Notice 21-327 Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto-Assets*' to provide guidance on the scope of regulatory oversight.
- On 27th January Singapore introduced a *Payments Services Act* requiring licences to permit trading.
- On 21st February the German regulator BaFin issued guidance confirming that Cryptocurrency issuers, regardless of where they are based, require licenses to operate within the country.
- On 23rd February the G20 reinforced its commitment to the Financial Action Task Force

(FATF) measures to reduce the risk posed by cryptocurrencies.

- On 24th February the Malaysian Securities Commission issued guidelines under s.377 of the Capital Markets and Services Act 2007 requiring platform operators to register.
- On 5th March South Korea passed legislation providing a framework for the regulation of currencies and exchanges which included oversight through licensing provisions.
- On 6th March the Supreme Court of India struck down the 2018 Reserve Bank of India's ban on financial institutions providing banking services to cryptocurrency businesses. The ruling, whilst opening up the capacity to trade, noted in particular the absence of regulation.
- On 9th March the "Crypto-Currency Act of 2020" was laid before the US congress: a bill which may well struggle to pass but marks an attempt to define the role and scope of crypto-currency regulation across the US market and beyond.
- On 1st April Russian authorities confirmed further delay in the "On Digital Financial Assets Bill" due to coronavirus. Whilst a ban on the use of cryptocurrency remains, the state bank confirms it is considering the promotion of a Russian-based digital currency.
- On 3rd April the Japanese government announced that legislation passed last year regulating cryptocurrency would be enforced from May 2020. As well as placing financial requirements on traders, the Financial Instruments and Exchange Act creates offences relating to the fraudulent sale, purchase, or trading of crypto-assets or derivatives.

Overall, the global trend towards greater regulation of crypto-currency platforms is undeniable and creates a significant challenge to those attempting to operate nationally or internationally in a competitive and often opaque marketplace. One positive interpretation is that greater regulation reflects and promotes greater recognition and acceptance: traders taking on the burden of regulation will also benefit from its hallmark. Such optimism is largely offset, however, by genuine concerns regarding how different national regulators will seek to enforce the rules and the extent to which there can or will be a level playing field.

To this end, in January the World Economic Forum saw the creation of the first Global Consortium for Digital Currency Governance: a grouping of financial institutions, governments, academics, companies and experts dedicated to providing effective guidance to national bodies on regulation and enforcement. Whilst given much fanfare and kind words, it is too early to see whether this will produce meaningful assistance to national regulators.

In the meantime international standards exist, at least notionally, with the G20 as recently as 26th February reiterating its commitment to the Financial Action Task Force (FATF) standards on virtual assets. The difficulty with these standards is the extent to which they depend and require national subjective risk assessments[3]. At present, cooperative international enforcement seems idealistic at best with the prospect that safe-havens of light-touch regulation could become the Cayman Islands or Switzerland of the digital era.

The UK and the FCA – Supervision

In the UK the initial framework for regulatory enforcement lies in the 5AMLD which provided new guidelines for digital currencies and a new, broader, definition than that previously encompassed by the 2015 European Central Bank guidance. Cryptocurrency, defined as any '*digital representation of value that can be digitally transferred, stored or traded and is accepted by natural or legal persons as a medium of exchange*', now faces the same AML and counter terrorism provisions as traditional banks and financial institutions.

With the introduction of the regulations, cryptocurrency firms and exchanges find themselves required to undertake customer due diligence and submit suspicious activity reports, and designated Financial Intelligence Units in each jurisdiction have gained the ability to collect the identities and addresses of virtual currency owners. Exchanges were required to register with national competent authorities with the overall aim of a European Register by September 2020.

In the UK, the FCA became the designated AML and Counter-Terrorist Financing Supervisor for crypto-asset activities following amendment of the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017. Prior to this it had already begun the process of regulation by publishing guidance on crypto-assets on 31st July 2019.

[3] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

The official approach of the FCA towards regulatory supervision is set out in that guidance:

> *'Our supervisory approach to cryptoasset businesses will be in line with our approach to other businesses under the MLRs. It will be risk based so that businesses who pose the greatest money laundering and terrorist financing risk will receive an increased level of supervisory focus. If we have reason to believe serious misconduct has taken place, we may decide to commence an enforcement investigation.'*

The level of 'risk' attributed to cryptocurrency by the FCA was recently highlighted in a speech on 6th March 2020 by its Director of Retail and Regulatory Investigations (Therese Chambers). In this speech Ms Chambers identified what the FCA views to be the inherent problem posed by cryptocurrencies, which often neither require nor rely on any regulated intermediary such as a bank or forex trader:

> '*Crypto-assets like bitcoin are a peer-to-peer technology and the settlement goes through an anonymous network of computers. The absence of an intermediary to authenticate a transaction presents particular challenges when applying financial crime regulation, designed for a market with intermediaries, to areas of the cryptoasset community.*'

The speech, whilst touching lightly on the potential social or financial benefits from a regulated crypto-asset system, focused more predominantly on the regulator's view that '*the risk of money laundering using crypto-assets is serious and real*'. On this basis it would appear a 'risk-based' supervisory approach is bound, at least in the initial stages, to lean towards a firmer hand.

To combat the level of perceived risk, the amended MLRs grant the FCA specific powers to investigate, prohibit and enforce legislative requirements, including:

- The ability to request information from any firm which is undertaking a cryptoassets activity covered by the regime. (Ref 74A)
- The power to impose a voluntary or involuntary requirement on a firm: a power so wide in scope as to be able to stop the business operating entirely if there is deemed to be a credible risk of money laundering. (Reg 74C)
- The authority to apply 'fitness' tests to individuals operating firms and the ability to 'request' the firm appoint an alternative. This includes the ability to require a crypto-asset business to appoint a 'skilled person' to prepare a report for the FCA concerning a matter under the MLRs (Reg 74B)
- The power to require disclosure to clients as to the risks of trading and where activity falls outside the protection of the Financial Services Compensation Scheme and/or Financial Ombudsman Service (which is nearly always).

For some, the application of existing models of regulation to cryptocurrency is uncomfortable and ill-fitting. Such people view the effect of the global tightening as being to undermine the ethos and purpose of digital currencies; a minority will find the principle of a central register unacceptable. The majority, however, recognise that as long as virtual transactions present and represent a genuine risk of abuse by criminal and terrorist organisations, there needs to be some form of regulatory control or oversight. The difficulty lies in creating regulations which preserve the benefits of virtual trading and pursuing enforcement in a manner which allows markets to develop and innovate without the threat of draconian punishments.

Enforcement: Stamping authority or stomping green-shoots?

On 3rd April 2020 the FCA closed a consultation on changes to the Enforcement Guide (EG) and Decision Procedure and Penalties Manual (DEPP) aimed to consider an extension of investigation and sanctioning powers to crypto-asset businesses under the MLRs. At present there is no published outcome of the consultation but it seems likely these will have a clear impact on those who fall within the scope of FCA regulation and the risk of enforcement.

It did not take long for the regulator to demonstrate that its powers are neither notional or reserved and some would argue the FCA have taken an overly-aggressive approach to what it clearly perceives as a risk-abundant industry.

In February 2020 an intervention by the FCA led to Epayments Systems Limited (ESL) suspending its trading and accounts. The FCA quickly updated the financial services register to require that ESL '*must not conduct business with corporate, individuals and/or freelance customers*.' Whilst there is not yet clarity as to the reason for the FCA intervention, ESL was known to be linked to a significant level of crypto-currency transactions. To put this in context, ESL is no small company or start-up exchange: at the time of its suspension it controlled over one million personal accounts and 1,000 business accounts and was issuing its own pre-paid cards through Mastercard. It is believed to hold in excess of £125 million of client funds. The role of the FCA and the purpose of the action was clear from the EPay announcement:

'*On February 11 epay systems Ltd agreed with the FCA to suspend all activity on its customers accounts. The decision was taken following a review, by the FCA of epayments anti-money laundering systems and controls which identified weaknesses that require remediation.*'

On 3rd March the FCA again took action against another platform, issuing a formal warning regarding BitMEX, which describes itself as 'Bitcoin's most advanced trading platform', asserting it was '*providing financial services or products in the UK without our authorisation*'.

Alongside the FCA's actions, the UK courts have shown themselves increasingly willing to deal with issues surrounding cryptocurrency trading and assets. In the civil courts recent cases such as *Robertson v Persons Unknown* (unreported, High Court Moulder J CL-2019-000444), *Vorotyntseva v Money-4 Limited* [2018] EWHC 2596 (Ch) and *AA v Persons Unknown 2019] EWHC 3556 (Comm)* have seen civil enforcement against cryptocurrency assets undertaken by, amongst other, the NCA. The criminal courts had already for some time *(R. V Teresko (Sergejs)* [2018] Crim. L.R. 81) determined such assets to be recoverable under section 84(1)(b) of POCA 2002 and prosecutors, including the FCA, are now regularly inviting seizure of cryptocurrency assets within confiscation orders.

Both the FCA and the Courts are, it would seem, gearing up to deal with potential prosecutions or enforcement actions relating to crypto-currency trading.

What to do?

Given the complexity and obscurity of the role played by some platforms, it will be important first to consider whether a company or individual falls within the (admittedly broad) scope of FCA 'regulated activities'. A starting point is the 'Guidance to Cryptoassets' (PS19/22) issued in July 2019 (subject to amendment and review in July 2020).

The guidance identifies the scope of those covered by reference to the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 as:

1) Cryptoasset exchange providers (including Cryptoasset Automated Teller Machine (ATM), Peer to Peer Providers, issuing new cryptoassets, e.g Initial Coin Offering (ICO) or Initial Exchange Offerings which is defined as:
   a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services.
   (a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,
   (b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or
   (c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.

2) Custodian Wallet Providers, which is defined as:
   a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer
   - *cryptoassets on behalf of its customers, or*
   - *private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets, when providing such services.*

If a business' or individual's actions fall within the definition of a regulated activity, then it is required to be registered with the FCA. The dates for required registration are different depending on whether it is a new business beginning operations after 10th January 2020 or an existing business which was trading in regulated activity before this date. All new businesses must be registered before any activity is carried out with existing businesses being registered by 10th January 2021.

Irrespective of whether the business/individual undertaking a regulated activity is formally registered with the FCA, it must comply with the MLRs. This will include being in a position to '*demonstrate that it has policies, controls and procedures in place to effectively manage money laundering and terrorist financing risks proportionate to the size and nature of the business' activities'*. The FCA will also expect that businesses will be in a position to demonstrate that they carry out regular assessments of their policies, controls and procedures to ensure that these remain relevant and appropriate and monitor operating models to identify increased risks.

The FCA provides a (non-exhaustive) list of requirements within the guidance:

- *take appropriate steps to identify and assess the risks of money laundering and terrorist financing which the business is subject to,*
- *assess the ML/TF risks related to any new technologies prior to launch and take appropriate measures to manage and mitigate those risks,*
- *have in place policies, systems and controls appropriate to mitigate the risk of the business being used for the purposes*

of money laundering or terrorist financing. This risk-based approach should seek to mitigate the risks identified in the business's risk assessment,

- *where appropriate with regard to the size and nature of its business, appoint an individual who is a member of the board or senior management to be responsible for compliance with the MLRs and the nominated officer. The nominated officer is also the person responsible for reporting suspicious activity to the National Crime Agency (NCA) under part 7 (money laundering) of the Proceeds of Crime Act 2002,*
- *where appropriate, with regard to the size and nature of its business, establish an independent internal audit function with responsibility for examining and evaluating the adequacy and effectiveness of the policies, controls and procedures, and making recommendations, as well as monitoring the controls,*
- *undertake screening of employees,*
- *undertake customer due diligence (CDD) when entering into a business relationship or occasional transactions,*
- *apply more intrusive due diligence, known as enhanced due diligence (EDD), when dealing with customers who may present a higher ML/TF risk. This includes customers who meet the definition of a politically exposed person (PEP),*
- *undertake ongoing monitoring of all customers to ensure that transactions are consistent with the business' knowledge of customer, the customer's business and risk profile.*

Ultimately, navigating the changing requirements of regulation, both within the UK and internationally, will represent a challenge to most crypto-currency providers. Whilst some will understandably shrink from (or bridle against) the imposition of regulatory oversight on a product and industry which was created specifically to be an independent alternative to traditional banks and financial products, there are others who are seeking to benefit from the recognition which regulatory compliance brings. DAG Global, a London-based company established in 2018, is understood to have resubmitted its application for a banking licence in March of this year with a view to providing bank accounts for crypto businesses. If it succeeds it will be the first British licenced provider of its type.

Despite what appears to be deep concerns on the part of the regulator as to the risks behind the operation of crypto-currency as a whole, it is difficult to see how licences could be refused to a compliant applicant. The benefit of a clear regulatory framework lies in the ability clearly to demonstrate compliance and it is possible the courts themselves, through the process of judicial review, could become a tool to enforce the right to trade as much as to enforce regulatory compliance. Cryptocurrency providers may gain significantly from understanding the system of regulation and turning it to their advantage.

In other financial crime news …

- It took the jury under 6 hours to bring to an end the long-running SFO's prosecution of Barclays executives in relation to the Bank's raising of funding from Qatar during the 2008 financial crisis. The acquittal came on 28th February 2020 at the end of the 5-month trial of the three remaining directors; Roger Jenkins, Tom Kalaris and Richard Boath. Former CEO, John Varley, had been acquitted last year and former finance director, Chris Lucas, did not face trial due to ill health..
- In better news for the SFO, on 31st January the Court approved a Deferred Prosecution Agreement ("DPA") between the SFO and Airbus in relation to the SFO's investigation of bribery allegations against Airbus in five jurisdictions (as part of a joint investigation with French and US authorities). The DPA, which was part of a €3.5bn global settlement by Airbus) involved the payment of €991m, to the UK authorities (€585,939,740 in disgorgement of profits, €398,034,571 by way of penalty and almost €7m is SFO costs).
- On 8th April, the High Court discharged three Unexplained Wealth Orders ("UWOs") and related Interim Freezing Orders ("IFOs") that had been granted on the ex parte applications of the National Crime Agency ("NCA") in relation to properties alleged to have been obtained with the proceeds of criminal conduct by the former Khazak President, Mr Rakhat Aliev. Finding in favour of Mr Aliev's daughter and grandson who asserted that the properties were funded though their own independent wealth, Mrs Justice Lang concluded that the NCA's conclusion that the funds came from Rakhat Aliev's unlawful conduct was "unreliable".

THE EFFECTS OF COVID-19 ON FINANCIAL CRIME AND COMPLIANCE

Written by Thomas Daniel

The true extent of the effects of COVID-19 on the world and the global economy may not be known for many years but it is well-known from past crises that each disaster brings a new opportunity for financial criminals to exploit.

Whether linked directly or indirectly, it is easy to see how the current pandemic could give rise to new types of offending and also that it will produce fresh considerations for regulated persons and corporate entities who are striving to remain legally compliant in unprecedented times.

Areas of likely offending by individuals

The types of individual offending linked to COVID-19 are likely to include:

(i) Scams: This outbreak has seen a surge in the use of technology by individuals, including vulnerable people who are using this technology for the first time. Predictably, there have already been numerous reports of individuals being the victims of cold calling or phishing scams, either designed to prey on their fears or their charitable nature by posing as health organisations;

(ii) Insider Dealing: With large, listed companies being affected in different ways, and staff members being similarly affected by the financial uncertainty, there is an increased risk that insiders may leak or trade upon material non-public information attributable to COVID-19 in an attempt to gain for themselves or to mitigate their losses (an allegation already raised against a number of US Senators);

(iii) Bribery: The virus has caused many countries to close airports and reduce staffing levels across customs borders and ports. Parties may be tempted to bribe public officials to circumvent procedures in order to get their goods through and officials in such roles may be more inclined to accept money to turn a blind eye; and

(iv) Counterfeit or sham goods: With the urgent need for medical supplies and Personal Protective Equipment being bought from foreign jurisdictions and from companies where there is not an established trading history between the parties, it is likely that consumers will fall victim to being provided with counterfeit or substandard equipment, or they will not receive the product purchased at all.

Are public bodies equipped to respond?

On 6 March 2020, Action Fraud stated that, since February alone, the National Fraud Intelligence Bureau had identified 21 reports of fraud where Coronavirus was mentioned, with victim losses totalling over £800,000. By 4 April 2020, this had reportedly risen to 509 reports, with losses in the region of £1.6m and victims were publicly complaining of the service they had received from the police and Action Fraud.

Coronavirus-related offending is not unique to the UK and it is clear, even in these early stages, that law enforcement bodies around the world are keen to be seen to be taking a proactive and tough stance towards criminality aimed at exploiting the pandemic. For example, on 22 March 2020, only nine days after President Trump declared a national emergency, the US Department of Justice announced that it had taken its first action in a federal court to combat fraud related to COVID-19 in relation to a website purporting to sell vaccines.[4]

What is less clear is whether the wish to be seen to be taking action will translate into investigation and prosecution of more than a handful of cases. On 19 March 2020, the Office for National Statistics released

[4] https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud

a publication on the nature of fraud and computer misuse for the year ending March 2019. The figures suggested that the number of frauds in England and Wales continued to rise. This had resulted in 3.8 million cases of fraud, although available statistics show there were only 7,725 offences which resulted in prosecution.

Notwithstanding the recognised difficulties associated with prosecuting financial crime, this announcement that approximately "one in 500 frauds" results in a prosecution (and not necessarily a conviction) could not come at a more striking moment, with the looming prospect of a spate of new financial crimes at a time when public resources are more stretched than ever.

So, what can be done?

In the first place, it goes without saying that consumers should be extra vigilant when dealing with unknown parties or parting with money, and they should make sure they request and retain documents concerning their dealings with all third parties. They would also be well advised to seek to corroborate any information about the other party from independent sources.

If the crime has already occurred, victims should continue to report matters to the police and via Action Fraud, even if others are doubting the effectiveness of these traditional routes at present. Law enforcement bodies continue to use various databases to cross-reference reports and intelligence, so reporting offences makes it more likely that large scale offenders will come to the attention of the authorities.

As an alternative, in recent years, many victims have resorted to bringing private prosecutions when public prosecutors have failed to act, and this may continue to be a useful option in certain circumstances.

Offences committed by individuals against individuals are, by their nature, likely to be more time-sensitive than investigations into corporates or those in the regulated sector, where record-keeping is presumed, the records are often highly probative, and the potential suspect is likely to be traceable. On the other hand, individual perpetrators are more likely to evade the authorities and disappear. In this sense, and with public resources under pressure, timely reporting of financial offences is likely to become even more critical.

When cases linked to COVID-19 inevitably start to work their way through the criminal justice system, it can safely be anticipated that judges will seek to introduce a strong deterrent effect by increasing sentencing for anyone who is deemed to have offended to take advantage of the current crisis, much in the same way the courts did during the 2011 riots, during previous financial crises and with frauds on Grenfell support schemes.

The impact on corporate offences of "failing to prevent" criminal activity

It is likely that corporates will also face increased exposure to the risks of failing to prevent COVID-19 related offending by individuals within or associated with the company. *Section 7* of the *Bribery Act 2010* provides that a commercial organisation will commit an offence if a person associated with it bribes another to obtain or retain business, or an advantage, for the organisation. The section provides that it is a defence for the organisation to prove that it had in place *"adequate procedures designed to prevent persons associated with it from undertaking such conduct."* Assuming the index bribery by the individual is proven, to establish this defence, the corporate would need to satisfy a reverse burden on the balance of probabilities.

More recently, *Part 3* of the *Criminal Finances Act 2017* created corporate offences for bodies failing to prevent the facilitation of tax evasion by persons associated with the body. In a similar fashion to the *Bribery Act 2010*, it is a defence for the body to prove that, when the UK tax evasion facilitation offence was committed: (a) it had in place such prevention procedures as it was reasonable in all the circumstances to expect that body to have in place, or (b) it was not reasonable in all the circumstances to expect the body to have any prevention procedures in place.

In February 2012, Guidance issued by the Secretary of State under *section 9* of the *Bribery Act 2010* identified six key principles for corporates to apply. These were: (1) Proportionate procedures; (2) Top-level commitment; (3) Risk Assessment; (4) Due Diligence; (5) Communication (including training); and (6) Monitoring and review. This is largely mirrored in HMRC's guidance published in September 2017 in response to *section 47* of the *Criminal Finances Act 2017*. The fact that the 2017 guidance repeated the *Bribery Act 2010* guidance from five years earlier reinforces that these are still the criteria against which corporate defendants will be judged.

HMRC has already faced criticism for the lack of prosecutions in the two years since the introduction of the *Criminal Finances Act 2017*. Whilst it has been announced that investigations are underway, this

legislation came into force at a time when HMRC was devoting a large amount of resources to Brexit-related matters and with COVID-19 now likely to occupy the headlines for months to come and other offences likely to be priorities, it remains to be seen how effective the enforcement of these offences will be.

What is clear is that the authorities are likely to be increasingly reliant on businesses policing themselves. Indeed, one of the aims of criminalising corporates for failing to prevent offences being committed by its staff or agents was to provide powerful incentives for corporates to take responsibility for detecting business crime within its four walls. As a matter of public policy, this is an acceptable position when it is apparent that a corporate body will have greater transparency and insight into its internal workings than external law enforcement. There are also benefits available to corporates who self-report.

In relation to tax offences, the effectiveness of tackling the underlying criminality has been undermined by public polls indicating that there is a low awareness of the existence of the 2017 offences amongst businesses. After all, if businesses are not alive to this legislation, it is unlikely that this will achieve the desired aim in the long term.

That said, the effects of COVID-19 are likely to make it harder for businesses to detect and prevent offending given that they are likely to be operating at a reduced capacity with staff (including compliance staff) working remotely. Whilst businesses may hope that the authorities and Courts will recognise this and make appropriate allowances, the view may well be taken that, with the authorities already overstretched, the need for businesses to self-regulate their staff and to report matters to the authorities is more important than ever.

The 2012 guidance indicated that the principles were intended to be flexible and that sentiment is likely to be heavily relied upon by businesses in light of the effects of COVID-19, particularly since some of the suggestions in the guidance and case studies are incompatible with the requirements of self-isolation and social distancing (for example, conducting face-to-face meetings with agents and the ability to verify documents). Where a company's preferred procedures cannot be followed, companies would be well-advised to see whether they can adapt or increase the measures that they do have in place to compensate for the loss of those rendered impossible by the current crisis. In respect of agents, this might include introducing additional verification checks until face-to-face meetings can safely resume.

Alongside making any enforced changes, many of the measures within the guidance are still capable of being fulfilled, although these will be performed remotely. For example, communication could be effectively carried out by interactive video conference and e-training courses are now an integral part of modern professional development.

Compliance and the regulated sector

Part 7 of the *Proceeds of Crime Act 2002 ("POCA")* creates offences for those in the regulated sector who fail to make a required disclosure if they know, suspect or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering and that information came to them in the course of their business in the regulated sector. With relationships with customers now necessarily being conducted remotely due to COVID-19, any assessment of whether there are "reasonable grounds" will be affected (as would any "reasonable excuse" defence).

On 12 and 31 March 2020, the European Banking Authority ("EBA") made a number of statements in relation to COVID-19. The EBA warned of the need to identify new and emerging risks and that monitoring transactions and suspicious patterns should be viewed in light of the customer's industry. The EBA noted that mitigating the effects of the pandemic may require temporary adjustments in supervisory activity and encouraged making full use of the flexibility embedded in the EU's AML/CTF framework in an effective, pragmatic and risk-sensitive way. The examples given included temporarily postponing non-essential onsite inspections and moving towards virtual meetings.

An important, time-critical issue is how regulated persons are to deal with the risks of money laundering in the course of business and how they are to approach their reporting requirements.

The Law Commission's 2019 Report entitled *"Anti-money laundering: the SARs regime"*[5] noted the increasing numbers of SARs and comments from the NCA that the current system was "untenable" in light of the continued increase. Furthermore, its observations

[5] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5569_LC_Anti-Money-Laundering_Report_FINAL_WEB_120619.pdf

included the fact that permission was actually refused in a small percentage of cases, the low quality nature of the information provided in some disclosures, the fact that the *Da Silva* test for suspicion was not met in a number of examples reviewed and that reviewing SARs in a time-sensitive manner, as the NCA must, is very resource-intensive.

For those in the regulated sector, any practical difficulties faced in relation to performing customer due diligence as a result of COVID-19 cannot be overcome by attempting to gain protection by simply making an authorised disclosure. The effect of taking this course would be notionally to lower the suspicion threshold and to abdicate the responsibilities imposed by POCA. Furthermore, in light of the Law Commission's findings from less than a year ago, a further surge in low quality SARs would not be productive and is likely to lead to delays with the NCA having to engage the moratorium period to deal with such reports.

On 4 March 2020, the FCA issued a statement on COVID-19, in which it stated that it expected all firms to have contingency plans in place and that it expected firms to *"take all reasonable steps to meet their regulatory obligations."* The statement made clear that if firms were able to meet their obligations from backup sites or with staff working from home, the FCA had no objection to this. The FCA also stated that it would be continuing its active dialogue with firms and that its guidance would be kept under review.

Therefore, at present, the FCA's approach is certainly that there will no immunity for firms and they are expected to adapt to the circumstances if they are to avoid enforcement. Unlike the time pressures associated with SARs, the powers available to the FCA would enable meaningful enforcement action to be taken after the peak of the pandemic.

From an AML/CDD perspective, in an ideal world, some financial institutions may wish to defer parts of their onboarding procedures until business returns to normal, however there is no support for this under the current regulations. Under *Regulation 30*, the relevant person must comply with the requirement to verify the identity of the customer, any person purporting to act on behalf of the customer and any beneficial owner of the customer before the establishment of a business relationship or the carrying out of the transaction. The exception within *Regulation 30(3)* states that, provided that the verification is completed as soon as practicable after contact is first established, the verification may be completed during the establishment of a business relationship but this is expressly restricted to instances where this is necessary not to interrupt the normal conduct of business and there is little risk of money laundering and terrorist financing.

Another obvious area of concern, with social distancing and self-isolation, is how firms are supposed to verify a client's identification when the client cannot produce certified copies face-to-face. On 31 March 2020, the FCA issued an open letter about COVID-19 to firms providing services to retail investors.[6] This noted that the FCA has received hundreds of requests for adaptations to its regulatory approach. Unsurprisingly, the FCA's position was that, whilst restrictions on non-essential travel have affected firms' abilities to use traditional methods to verify a customer's identity, client identity verification is an obligation under the *2017 MLR* and the FCA still expects firms to comply, although firms can be flexible in how they achieve this. The FCA reminded firms that the Regulations and JMLSG guidance already provide for client identify verification to be carried out remotely and that there are safeguards and additional checks firms can use to assist with verification, including seeking corroboration from lawyers or accountants, 'triangulating' geolocation data such as phone numbers and IP addresses, and even requesting clients provide 'selfies' or videos.

Following this, on 1 April 2020, the FATF President made a statement in relation to COVID-19 and the measures to combat illicit financing.[7] This encouraged the fullest use of "*responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures."* The statement also drew specific attention to the recently released Guidance on Digital ID,[8] issued as recently as March 2020, and called upon countries to explore using digital identity. The statement also encouraged the use of simplified due diligence when firms had identified lower money laundering risks.

[6] https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-coronavirus-update-firms-providing-services-retail-investors.pdf

[7] https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

[8] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

In practice, as the guidance suggests, it is likely that steps taken to obtain the best quality evidence of verification from a remote standpoint will mitigate against the risks now faced as a result of COVID-19.

For the purposes of verification, firms should review and, if appropriate, tighten their existing systems to compensate for any restrictions caused by the pandemic. This might involve checking whether the verification systems draw on multiple sources which are independent of each other. Furthermore, obtaining verification from official sources or sources which are secure from tampering will further mitigate any risk. Even if this is already the case, firms may wish to include an extra layer of verification to increase the reliability of the data it holds until it can revert to its usual procedures.

As firms can reasonably expect social distancing measures to be implemented for some time, or at least to be relaxed and then reinstated to manage the peak and spread of the virus, it would be wise to ensure that systems are capable of ensuring that AML paperwork is accessible from a remote location, where it can be accessed by relevant staff.

Conclusion

In these extraordinary times, corporates and those in the regulated sector should continue to apply the fundamental principles underlying their corporate governance and compliance procedures, albeit the method of achieving these aims may need to temporarily change to take account of the new challenges faced.

Constant monitoring, critical review and approaching compliance in a "thinking manner" will naturally enable the most innovative solutions to prevail. If these prove to be effective and cost-efficient, a silver lining to emerge from this disruption may even be that the introduction of new technology will replace outdated methods when business eventually returns to normal.

SANCTIONS: LESSONS LEARNED AND LOOKING AHEAD

Written by Rhys Rosser

On 18th February 2020, following a review under s.147 of the Policing and Crime Act 2017, the Economic Secretary to the Treasury upheld the decision of the recently established Office of Financial Sanctions Implementation ("OFSI") to impose monetary penalties against Standard Chartered Bank ("Standard Chartered") totalling £20.47m (a reduction from the original OFSI fine of £31.5m). Whilst this is dwarfed by the $947m payment to American agencies, it provides a reminder of the importance of UK sanctions compliance.

In providing financial facilities to a wholly owned subsidiary of Sberbank, the private Bank Denizbank, Standard Chartered breached sanctions imposed on Russian institutions and individuals involved in the annexing of Crimea and subsequent threats to the territorial integrity of the Ukraine. The purpose of the restrictions had been to limit access to Capital Markets and lending facilities.

Standard Chartered had already been investigated by the FCA who imposed a civil penalty of £102.16m on them for AML failings in January 2019. The FCA found that the inadequate due diligence, insufficient customer information and lack of ongoing monitoring exposed the bank to sanctions evasion and money laundering risks.

One area of particular concern was in relation to Standard Chartered's failure properly to monitor access to their Internet Banking in the UAE. The bank had been aware of this issue since 2010 but it was not until 2014 that they shut down the access. This is perhaps a salutary lesson in the importance of geo-tagging and having proper measures in place which restrict the use of IP address masking. This is a particularly pertinent issue at present due to the decreased lack of customer contact as a result of the Covid-19 lockdown.

Of course, whilst the OFSI proceedings against Standard Chartered were under the EU regulations (which remain in place until 11pm on 31st December 2020), once the UK exits the European Union, the Sanctions and Anti-Money Laundering Act 2018 ("SAMLA") will come into effect. This will represent yet another substantial change to the UK sanctions regime, with SAMLA giving the UK the power to implement autonomously new sanctions as well as lifting/updating existing ones.

The new regulations are drafted with a 'thematic' approach as well as being divided by jurisdiction; the current proposal is for the UN sanctions to form the Consolidated List with further additions made on an ongoing basis. The four themes that have been identified in advance are:

- Chemical Weapons
- Counter-Terrorism (Domestic)
- Counter-Terrorism (International)
- Isil (Da'esh) & Al-Qaida

The UK will effectively adopt a stand-alone sanctions regime, rather than being driven by the EU. As part of the introduction of SAMLA, the UK will adopt a 'Magnitsky Law' to deal with those suspected of human rights abuses and violations. The Magnitsky Act allowed the US authorities to quickly freeze the property interests of 17 individuals suspected of involvement in the alleged murder of Jamal Khashoggi in Saudi Arabia. The EU are yet to adopt such legislation – this is one of the first signs that the UK's approach to sanctions will be more closely aligned with the US than Europe in the coming years.

The UK's commitment to maintaining and increasing Sanctions monitoring after the exit from the European Union is typified by The Russia (Sanctions) (EU Exit) Regulations 2019. These regulations are likely to be substantially the same as the EU provisions, but with scope to change as the situation in Russia, and Ukraine, develops. The UK are effectively on the front foot to build a more flexible, and likely more intensive, sanctions regime for businesses once Brexit truly begins.

This independence is reflected in the new approach to ownership and control, determining whether a designated person, i.e. those subject to sanctions, is linked to a company/institution. SAMLA will also provide for the granting of 'General Licenses' which allow multiple parties to engage in activities which would otherwise result in a breach of sanctions. This approach to licensing is already widely employed in the US and again demonstrates the closer mirroring of the US regime.

However, the freedom created by the UK's individual approach allows the flexibility to be divergent from the US where necessary. This is demonstrated by the proposed Regulations in respect of Iran which align with the EU, whilst the Russian Regulations more mirror the US approach.

There are clearly lessons that can be learned from the treatment of Standard Chartered by the OFSI and the approach taken by UK Officials to SAMLA.

Customer Due Diligence is likely to be closely monitored an ongoing basis, particularly given the tendency for large organisations to outsource their KYC and onboarding checks. The implementation of a policy is going to be the focus of investigations, rather than simply whether the policy is sufficient. This will more closely reflect the adequate procedures test set out in the 2010 Bribery Act.

The financial penalties imposed on Standard Chartered demonstrate the importance of ensuring Sanctions Policies are up to date and pro-active monitoring takes place.

What is also clear is that OFSI are going to reflect voluntary disclosure with substantial reductions in penalties: commencing internal reviews and investigations at any early stage will continue to pay dividends. Voluntary disclosure was reflected in the 30% reduction applied to the financial penalties imposed on Standard Chartered (as a result of the severity of the breach, the usual 50% reduction was not applied). It should, however, be remembered that OFSI remains a relatively new organisation, so principles and policies are rapidly changing.

The Chambers of Brian Altman QC & Jim Sturman QC is continuing to operate and our barristers are available to accept instructions (but can only attend Court where safe to do so and in accordance with current restrictions). However, in the current state of emergency in relation to Covid-19, Chambers premises are closed and all staff are working remotely. For obvious health reasons we are not accepting the delivery of hard copy sets of papers, we ask that you send soft copies via a scan or a zip file, or use some other electronic media platform such as Dropbox or your preferred method for large volumes of papers.