THOMSON REUTERS
PRACTICAL LAW™

King & Spalding: transatlantic business crime and investigations November column

by Andrew Michaelson (New York), Brandt Leibe (Houston), William T Gordon (Washington D.C.), Aaron Stephens (London), Rob Dedman (London), Katie Barry (New York), Jacob Gerber (New York), Liam Petch (London), Caspian Heeler (London), Joanna Harris (London), King & Spalding

Status: **Published on 10-Nov-2020** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-028-1903**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

King & Spalding's Special Matters and Government Investigations team shares its views on developments in transatlantic business crime and investigations.

Prosecution of commercial bribery outside the US: does honest services fraud represent a new frontier in DOJ enforcement?

A federal appeals court in the US recently affirmed a remarkable result: the criminal conviction of foreign individuals, working for foreign institutions, for commercial bribery. Historically, the US Department of Justice (DOJ) has focused on foreign **public** corruption, and indeed the US Foreign Corrupt Practices Act (FCPA) is cabined to conduct involving corrupt payments to foreign officials. To reach commercial bribery, prosecutors could not use the FCPA. Instead, prosecutors turned to the controversial honest services fraud statute, and in *United States v Napout*, 963F.3d 163 (2d Cir. 2020) the US Court of Appeals for the Second Circuit affirmed the use of that statute to prosecute foreign commercial bribery. They did so even though the defendants both lived and worked in a country where commercial bribery is non-criminal. For more information on the FCPA see Practice note, The Foreign and Corrupt Practices Act: Overview.

Napout is significant. Corporations can no longer assume that the DOJ will investigate foreign bribery only if a public official is involved. While those with a UK nexus will already be alive to the risk of the UK Serious Fraud Office (SFO) prosecuting foreign commercial bribery under the Bribery Act 2010, *Napout* arguably reflects broader reach given that neither the individuals nor their employers were located in the US. For more information on prosecuting bribery in the UK see Practice note, Bribery Act 2010. Following *Napout*, US prosecutors can charge foreigners working for foreign institutions for commercial bribery so long as the use of US wires, such as wire payments or electronic communications, are an integral part of the scheme.

United States v Napout: decision

Set against the backdrop of a highly publicised and wide ranging enforcement effort against several international soccer officials, in *Napout* the US Attorney's Office for the Eastern District of New York (EDNY) indicted and sought conviction of two individuals from South America: Juan Ángel Napout, the former president of CONMEBOL (the South American soccer confederation), and José Maria Marin, the former president of CBF (the Brazilian soccer federation) (together, the appellants). Neither CONMEBOL nor the CBF are government entities. The indictment accused the appellants of accepting millions of dollars in bribes each in return for awarding lucrative broadcasting and marketing rights for international soccer matches, including the Copa America and Copa Libertadores tournaments.

EDNY obtained convictions of the appellants for conspiracy to commit honest services wire fraud, which is an offence due to the interplay among three statutes: the US wire fraud statute (18 United States Code (USC). section 1343), the honest services fraud statute (18 USC section 1346), and the wire fraud conspiracy statute (18 USC section 1349). Taken together, these statutes prohibit conspiring to devise a scheme or artifice to deprive another of the intangible right of honest services, by a wire. The Second Circuit's affirmation is notable because:

- The accusations related to **commercial bribery**, with no government bodies or public officials involved in the schemes. Commercial bribery is not criminalized under the primary tool for prosecuting foreign bribery in the US, the FCPA.
- The appellants were foreign individuals (Paraguayan and Brazilian) who worked for foreign entities. Honest services fraud can occur where an employee breaches a fiduciary-like duty owed to his or her employer. Here, prosecutors contended that a Code of Conduct promulgated by FIFA and adopted by CONMEBOL

and FIFA imposed the requisite duty on appellants. Therefore, a private, foreign organization's code of conduct created a fiduciary-like duty, the breach of which gave rise to criminal liability in the US for honest services fraud (even though commercial bribery is not criminal in either Paraguay or Brazil).

- The appellants' actions were not directed at the US, and the scheme took place largely in South America. The Second Circuit concluded, however, that the "conduct relevant to the statute's focus," that is, the use of US wires and financial institutions was "integral to the transmission of the bribes" in the alleged foreign scheme and that therefore, the convictions should be affirmed.

US: foreign commercial bribery under the FCPA

The FCPA is limited in that it criminalizes payments to foreign government officials for the purpose of obtaining, influencing or retaining business. The anti-bribery provisions of the statute make it unlawful to give or offer any corrupt payments to "any foreign official" or to "any foreign political party or official thereof, or any candidate for foreign political office".

- The FCPA is also focused specifically on companies and persons operating in the US: the anti-bribery provisions apply to both: US securities issuers, which are companies that have securities registered in the US or are otherwise required to file periodic reports with the SEC. "Domestic concerns" which include citizens, nationals, and residents, as well as most business organizations with their principal place of business in the US or organized under the laws of any particular state.

The FCPA can also apply to foreign persons, but only if they or their agents engage in corrupt payments while in the territory of the US (the territorial jurisdiction provisions).

The intent to limit the scope of the FCPA was clear in its text and legislative history: early FCPA proposals in both the House and Senate specifically addressed bribes to nongovernmental parties. However, Congress in 1977 omitted private bribery from the final act, reporting that it "fully recognizes that the proposed law would not reach all corrupt payments overseas". Therefore, it was clear from the outset that the FCPA would focus solely on foreign public bribery. It is similarly clear from the legislative history that Congress intended to impose limits on criminal liability of foreign persons under the FCPA.

Eleven years later, in 1988, Congress passed the honest services fraud statute. The Supreme Court declared the statute vague in *United States v Skilling (2010), 561 U.S. 358 (2010)* and has ruled that it must therefore be construed in a manner that is consistent with Congressional intent, and only to the extent fair notice of its reach was provided to the public. It is therefore noteworthy that the legislative history of the honest services fraud statute does not reflect any intent by Congress to criminalize what they did not criminalize in the FCPA: foreign commercial bribery. The *Napout* decision expands the DOJ's reach over foreign conduct even in the absence of a statute explicitly criminalizing foreign commercial actors operating abroad.

UK: foreign commercial bribery under the Bribery Act 2010

The Bribery Act 2010, in contrast to the FCPA, criminalizes commercial bribery. The offences of bribing another person and of being bribed (the section 1 and section 2 offences, respectively) apply equally to activities carried out in the private sector and business functions and activities. However, these offences only apply to actions or omissions within the UK, or where a person has a close connection with the UK. A foreign individual acting abroad, and with no close connection to the UK, cannot be prosecuted pursuant to these offences.

However, the corporate offence of failing to prevent bribery (section 7 offence) applies with far broader territorial reach; it applies to companies incorporated in the UK or those that do any business in the UK, regardless of whether the relevant act or omission took place in the UK. This means that foreign companies that do business in the UK may incur liability by failing to prevent an associated person committing commercial bribery outside of the UK. Crucially, it is irrelevant for the purposes of this offence whether the associated person has a close connection to the UK.

The SFO has shown a willingness to pursue commercial bribery aggressively, making use of the broad reach of the section 7 offence. For example, the settlement earlier this year between Airbus S.E. and the SFO (which we reported on here on 14 April 2020 and which took place in tandem with settlements with US and French authorities) is an illustrative example; several the counts brought by the SFO under the Bribery Act 2010 were for foreign commercial bribery.

Conclusion

Napout provides stark notice that, for overseas individuals and companies, the risk of US enforcement for bribery and corruption is by no means limited to public corruption. Further, given the potential breadth of the conduct criminalized by the honest services fraud statute and the willingness of the DOJ to prosecute cases with an arguably tangential

US nexus, *Napout* reflects a noteworthy expansion of the DOJ's enforcement activity. Considering the enforcement powers of the DOJ and the SFO, businesses should accordingly take significant care in managing commercial bribery risk regardless of local laws.

Without prejudice to these words of caution, we note that a degree of doubt remains over the sustainability of the decision reached in *Napout.* The Second Circuit held that a key argument of the appellants that, under *Skilling*, the unconstitutional vagueness of the honest services fraud statute forecloses prosecutors from using it to enforce commercial bribery by a foreign individual working for a foreign entity, had not been raised before the trial court. It therefore considered that argument under a lower standard of review, concluding that it would not be "plain error" to use the honest services fraud statute in this manner. In a future case, or at the Supreme Court, the door remains open to challenge the use of the honest services fraud statute to prosecute foreign commercial bribery.

What the FinCEN leak reveals about the SAR regime on both sides of Atlantic

The leak of the "FinCEN files" last month has again thrown the spotlight on the suspicious activity report (SAR) regime and its effectiveness in preventing global financial crime. Of the 2,657 documents leaked, most are reportedly SARs filed to the US Financial Crimes Enforcement Network (FinCEN) concerning transactions worth more than $2 trillion that took place between 1999-2017. While the leaked documents were shared with the US authorities, British companies were named in the SARs more than entities from any other country. Both the UK and the US have similar SAR regimes and the impact of the leak is already being considered across both sides of the Atlantic by firms and regulators alike.

US and UK SAR regimes: a similar approach

Under the US Code of Federal Regulations, a bank must submit a SAR if it suspects or has reason to suspect a transaction involves funds derived from illegal activity or is attempting to conceal assets or funds derived from criminal activity. A SAR must also be submitted where a bank suspects or has reason to suspect that a transaction is designed to evade any provisions of the Bank Secrecy Act (BSA), or where a transaction has no apparent business or lawful purpose. Banks cannot be held civilly liable for naming a client or any other person in a SAR report - this is consistent with other protections afforded to witnesses and victims communicating with regulatory and criminal authorities. US law also requires other regulated financial entities, including broker-dealers and money service businesses, to file SARs under similar circumstances.

In the UK, the Proceeds of Crime Act 2002 (POCA) requires that a person must submit a SAR to the National Crime Agency (NCA) if they know or suspect, or have reasonable grounds for knowing or suspecting, a person is engaged in money laundering or terrorist financing. For more information on the UK SARs regime see, Practice note, Reporting suspicious activities: overview. All employees within the regulated sector, as defined by POCA, have reporting obligations where they have requisite knowledge or suspicion of a potential POCA offence. While there is no statutory definition of "suspicion", judicial guidance has confirmed that there must be "a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice" (*R v Da Silva* [2006] EWCA Crim 1654). This individual duty can be discharged by making an internal disclosure to a bank's Money Laundering Reporting Officer (MLRO), who is then obliged to consider whether the activity should be reported to the NCA. While organisations in the regulated sector are under a positive obligation to file SARs, the submission of a SAR to the NCA which seeks consent for a specific activity or transaction can also provide banks with a defence from the principal money laundering offences under POCA, provided they do not execute the transaction until they receive actual or deemed consent from the NCA. Where a SAR is made in good faith, case law has also determined that the bank will be protected from any civil liability arising from the failure to carry out a customer's instructions under a contract while they wait for that consent.

To prevent the hindrance of any law enforcement investigations, both the US and UK SAR regimes prohibit individuals who are filing (or have already filed) a report from disclosing any information about the existence, or the contents, of that report. This seeks to avoid "tipping off" the persons and entities identified in a report that the authorities have been apprised of their potential misconduct, with the assumption that this could invite efforts to conceal wrongdoing. In the US, the unauthorised disclosure of a SAR is a violation of federal law that carries civil penalties of up to $100,000 and criminal penalties of up to five years imprisonment and a $250,000 fine. In the UK, it is a criminal offence under POCA to disclose any information that would be likely to prejudice any enforcement investigation. The maximum sentence for a tipping off offence under POCA is two years' imprisonment in addition to a fine. The source of the FinCEN Files leak is not yet known, but FinCEN has referred the matter to the DOJ and the US Department of the Treasury's Office of Inspector General for investigation.

Spotlight on the SAR regime

Beyond the headline-grabbing stories alleging that prominent individuals moved funds through major banks to avoid international sanctions, the fact of banks and other financial institutions filing SARs is in fact a high-level indication that the industry is considering, and reporting, transactions where firms have the requisite knowledge or suspicion.

Some reports have suggested that banks are filing SARs with an insufficient level of detail to allow further investigation; however, many of the banks named in the FinCEN files have pointed out in public statements that the leaked documents relate to historical practices and note that much has since been done to improve internal procedures and controls. Since the Panama Papers, steps have also been taken by the relevant authorities in both the US and UK to increase the transparency of financial transactions and to improve the effectiveness of SARs for law enforcement agencies. For example, the Law Society published updated guidance on how to report suspicious activity to the NCA on 17 December 2019 and the NCA published guidance and FAQs on SARs as recently as March 2020. For more information see Legal update: Law Society's updated SAR guidance and Legal update: NCA publish guidance and FAQs on SARs.

However, another issue under the spotlight is the sheer number of SARs filed every year. In 2019, over 2.75 million SARs were submitted to FinCEN and between April 2018 and March 2019, over 478,000 SARs were submitted to the NCA. On one hand, given the relatively low legal threshold for determining "suspicion", it is perhaps unsurprising that the financial services industry files a significant number of SARs. On the other hand, there are persistent reports of institutions filing "defensive" SARs (to protect their own position) and the significant volume of SARs places a substantial burden on law enforcement agencies. There has been a near universal recognition that the SAR system as it currently exists is imperfect; the sheer volume of information makes it difficult for the authorities to separate the useful SAR from the defensive. Consequently, the question of reform of the SAR system has been a regular topic of debate on both sides of the Atlantic. However, it is noteworthy that in the UK the government is yet to implement any of the reforms to the SARs regime proposed by the Law Commission its report in 2019. That report recommended, amongst other things, However, it is noteworthy that in the UK the government is yet to implement any of the reforms to the SARs regime proposed by the Law Commission. For more information see Legal update: Law Commission report on the SARs regime.

Wider implications

In both the US and UK, there has been implicit acknowledgment of the issues raised by the FinCEN leak. On 16 September 2020, FinCEN announced its intention to enhance the effectiveness of its anti-money laundering programme by introducing potential regulatory amendments under the BSA. There have also been fresh calls from US policymakers, asking Congress to pass stalled legislation that would make it easier for banks to share information of suspicious activities without breaching privacy laws.

On 18 September 2020, the UK government announced plans to introduce compulsory identification verification at Companies House to help trace people committing money laundering or fraud. The Treasury Select Committee has since launched a fresh anti-money laundering inquiry, asking government, HM Revenue & Customs and the Financial Conduct Authority a series of questions on the fallout from the FinCEN leaks, including clarification as to what steps are being taken to further secure the financial system from economic harm.

The leak may also prompt further enquiries and potentially investigations from authorities outside of the US, particularly if a SAR has not been filed in the relevant jurisdictions. In the UK, the SFO and National Economic Crime Centre have already confirmed that they are in the process of determining if any action is required. Affected banks would be well advised to go back over the leaked data to ensure that they have carried out their regulatory responsibilities appropriately in non-US jurisdictions.

Conclusion

While public interest in the FinCEN leak will likely lead to further scrutiny of the role of the financial services industry in preventing global money laundering and other financial crimes, it also raises questions about the effectiveness of the system itself and the ability of enforcement agencies to use the significant volumes of data sitting within their SAR systems to identify, investigate and interdict potential financial crimes. Achieving this will require not only significant focus on reform of the SAR regime, but also an open and realistic discussion about both the budget of the various enforcement agencies and the historic policy of outsourcing to the financial services industry via legislation.

World Bank integrity vice presidency continues robust enforcement in 2020

On 8 October 2020, the World Bank Group (WBG) issued its Sanctions System Annual Report for the fiscal year 2020 (SSA Report), detailing the WBG's efforts to investigate and adjudicate allegations of sanctionable practices by firms and individuals in WBG-financed contracts.

In the fiscal year 2020, the WBG temporarily suspended 30 firms and eight individuals and debarred 46 firms and individuals. The SSA Report further highlights that in fiscal year 2020 the WBG's investigative and prosecutorial arm, the Integrity Vice Presidency (INT), received 2,958 complaints and opened 46 new external investigations.

The WBG continues to focus on meeting the needs of its constituents, including those caused by the unprecedented 2019 novel coronavirus disease (COVID-19) pandemic. However, INT makes clear that it maintains its robust investigation capabilities and that the pandemic will not prevent it from continuing to safeguard WBG resources.

Other key statistics include that:

- The INT submitted 26 cases and 22 settlements to the Office of Suspension and Debarment (OSD), the first tier of the two-tier Sanctions System.
- OSD sanctioned 19 respondents via uncontested determinations;
- The Sanctions Board, the second tier of the two-tier Sanctions System, issued six public final decisions.
- The Integrity Compliance Office engaged with 107 sanctioning parties towards meeting their conditions for release and determined that 18 sanctioned parties had satisfied their conditions for release.

The WBG also reported 11 external referrals, most to specific governments or government agencies, with the SSA Report stating that certain referral information was omitted where INT is aware of ongoing law enforcement action. When the WBG finds evidence of possible criminal conduct, it takes the view that it has a responsibility to make such referrals to its constituents. Without question, referrals increase the potential of parallel government investigations into suspected wrongdoing.

Those involved in WBG-funded projects must therefore remain vigilant and ensure compliance with all WBG requirements, including those enforced by INT. This includes trying to identify potential issues as early as the request for proposal and contracting stages; prevention is the best approach.