KING & SPALDING TRANSATLANTIC BUSINESS CRIME AND INVESTIGATIONS COLUMN

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

by *Aaron Stephens* (London); *Hayley Ichilcik* (London); *Joanna Harris* (London); *Kyle Sheahen* (New York); *Margaret McPherson* (New York); *Courtney Roldan* (Chicago); and *Blythe Kochsiek* (Los Angeles), King & Spalding

RESOURCE INFORMATION

RESOURCE ID

w-016-3313

RESOURCE TYPE

Article

PUBLISHING DATE

29 August 2018

CONTENTS

UK FOLLOWS US MOVES TO OBTAIN ELECTRONIC DATA OVERSEAS

In March 2018, the US Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), enabling the US to conclude international agreements through which foreign governments can seek data directly from US companies without each request having to go through the US government. Now the UK is following suit with its own version, the Crime (Overseas Production Orders) Bill (COPO Bill), which is currently proceeding through Parliament.

The alignment of the two statutory regimes creates the prospect of the two countries agreeing to bypass existing mutual legal assistance mechanisms in relation to electronic data. Such an agreement would exponentially speed up the process by which US and UK authorities can obtain electronic evidence held in each other's jurisdiction, where the requirements of the relevant local legislation are met.

However, it is important to note that the COPO Bill does not in itself enable the making of such an order; if enacted, it would only allow the UK government to enter into international agreements with other countries which permit this to happen. So far, no such agreement has been entered into.

What does the COPO Bill do?

If enacted, the COPO Bill will provide a statutory framework for the UK to collect electronic evidence stored outside the UK without the involvement of the authorities in the country where the evidence is stored.

Currently, to collect data from a service provider or other entity abroad, the UK would need to make a request for mutual legal assistance to the relevant government. As the explanatory notes to the COPO Bill point out, this is not always a quick process and sometimes the evidence does not arrive in time to be used. The COPO Bill envisages an overhaul to this system, with UK law enforcement agencies being able to apply directly to the UK courts for an order with extra-territorial effect. There are a number of safeguards built into this process and the courts would only be able to grant an overseas production order in specified circumstances. In particular, the judge considering the application would need to be satisfied that, amongst other things:

- There are reasonable grounds for suspecting that an indictable offence has been committed and that proceedings in relation to that offence have been instituted or that it is being investigated, or alternatively, the order is sought for the purposes of a terrorist investigation.
- The data is likely to be of substantial value to the criminal proceedings or the investigation in relation to which it is requested.
- Production of the data would be in the public interest.

These final two elements, in particular, reflect the requirements for obtaining domestic production orders under the *Proceeds of Crime Act 2002* (POCA 2002).

As with most regimes for compulsory production of documents in the UK, privileged material would not have to be provided. However, in addition and reflecting current data protection concerns, confidential personal records are excepted from production other than in the context of terrorism investigations. The explanatory notes to the COPO Bill give medical records as an example of such a record. In the context of orders against a telecommunications provider, data relating to the communication rather than its content are also excepted.

Another interesting aspect of the COPO Bill is that the judge can include a non-disclosure requirement in the order. This would prevent the person against whom the order is made from disclosing the fact or content of the order except with leave of a judge or the person that applied for the order. Question marks over enforceability will no doubt arise.

Why has the COPO Bill been introduced now?

There is an obvious synergy with the CLOUD Act passed in the US. Indeed, it appears the US was very much in mind; the House of Lords briefing document specifically refers to the fact that data sought by the UK authorities is often stored in the US and that the UK has been negotiating a bilateral data-sharing agreement with the US since 2015.

However, there is a broader impetus behind the COPO Bill: the government is clearly trying to keep abreast of the realities of law enforcement and evidence collection in the digital age. The cracks in older legislation have become clear over time. The CLOUD Act stemmed in part from the Microsoft warrant case and there are also current actions in the UK relating to the extra-territorial effect of the SFO's powers under section 2 of the Criminal Justice Act 1987.

What concerns have been raised?

The COPO Bill is not law yet; it will have a third reading in the House of Lords (where it was introduced) before moving on to being debated in the House of Commons.

During its second House of Lords reading, various concerns were raised, such as enforceability. Furthermore, while the checks and balances built into the process at the UK's end were noted (amongst other things, that the data must be of substantial value to the criminal proceedings or investigation for which it is being requested) a question mark was raised over how the UK would ensure that any reciprocal arrangements allowing other countries' orders to have extra-territorial effect in the UK would adequately safeguard UK entities.

What is the impact on companies?

Nothing, until the COPO Bill is enacted and a relevant international agreement entered into. However, once the powers envisaged by the Bill are in use, those under investigation will find that, generally speaking, the authorities will have quicker access to their data stored abroad, particularly if held by a well-known telecommunications provider; these companies will in turn likely face an onerous burden in trying to comply with this new species of order, including ensuring confidentiality where a non-disclosure requirement is included. However, the issue of enforceability may prevent the tool being effective against less conscientious targets.

The bigger picture is that companies should expect governments to seek more and more ways to access their data and to close any perceived loopholes in current legislation. Law enforcement agencies would clearly wish to have seamless access to data globally; the question is whether governments can reach agreements quick enough to make that a reality.

RISE OF FOREIGN WHISTLEBLOWERS IN US ENFORCEMENT

As financial transactions flow across borders with more speed and broader scope than ever, US law enforcement agencies continue to use every available tool to uncover potential misconduct. This includes encouraging whistleblowers to come forward with evidence of wrongdoing, wherever in the world they might be.

On 16 July 2018, the US Commodity Futures Trading Commission (CFTC) announced its first ever award to a non-US whistleblower. The CFTC awarded over $70,000 to an individual living in a foreign country who provided material assistance in an investigation. The CFTC's Director of Enforcement, James McDonald, remarked that the "award is significant because it signals to whistleblowers around the world that anyone with information about potential violations of the Commodity Exchange Act can participate in the CFTC's Whistleblower Program."

While this award is the first to a foreign whistleblower for the CFTC, other US law enforcement agencies have sought assistance from abroad for years. Perhaps most notably, former Swiss banker Bradley Birkenfeld received $104 million from the US Treasury in 2012 for the assistance he provided to the Department of Justice (DOJ) and the Internal Revenue Service (IRS) relating to offshore tax evasion at UBS. While Birkenfeld was himself an American, the conduct at issue involved Swiss private bankers assisting American taxpayers with hiding money offshore. The deferred prosecution agreement in that case required UBS to provide the US government with the identities of certain US customers of UBS' cross-border business, as well as those individuals' account information. By divulging information about UBS' conduct to the US government, Birkenfeld was able to obtain his massive award. However, his involvement in the scheme itself resulted in a stay in federal prison.

In September 2014, the US Securities and Exchange Commission (SEC) awarded a foreign whistleblower more than $30 million for information leading to a successful enforcement action. The SEC announced that the size of the award was due to this whistleblower's ability to provide "key original information" that led to the discovery of fraud that otherwise would have been "very difficult to detect". Even though the award was the largest SEC whistleblower award at that time, the SEC indicated that there was a downward adjustment due to the individual's delay in reporting the conduct to the SEC. Sean McKessy, the former chief of the SEC's Office of the Whistleblower, commented that the award demonstrated the "international breadth" of the SEC's whistleblower program and that the agency would continue to "effectively utilize valuable tips from anyone, anywhere".

More recently, in December 2017, the SEC awarded more than $4.1 million to a former company insider who alerted the SEC to a "widespread, multi-year securities law violation". The whistleblower was commended by Jane Norberg, current chief of the SEC's Office of the Whistleblower, when she noted that a "foreign national working outside of the United States, affirmatively stepped forward to shine a light on the wrongdoing". Norberg added that company insiders are the ones that have the information necessary to "help the SEC halt an ongoing securities law violation and better protect investors".

Government agencies have also rewarded foreign whistleblowers that brought allegations under the US False Claims Act. Dinesh Thakur, an India-based former executive of a generic drug manufacturer, brought a qui tam action relating to the manufacturing and distribution of adulterated drugs made in facilities in India. Under the Food, Drug and Cosmetic Act, drugs traveling through interstate commerce cannot be adulterated, and the company's failure to manufacture FDA-approved formulations led to false claims for those drugs to be submitted to Medicaid, Medicare, and others. In 2013, the drug manufacturer agreed to pay $500 million to resolve the false claims allegations (among other charges) based on the whistleblower's action, for which he was awarded approximately $48 million.

The upshot is clear: whistleblower programs of the US government have incentivised the reporting of violations of US laws by individuals around the world. Indeed, in its 2017 annual report to Congress regarding its whistleblower program, the SEC stated that it received whistleblower submissions from individuals in 72 foreign countries. This trend is expected to continue as law enforcement efforts become more co-ordinated around the globe.

The UK has considered (but so far ruled out) introducing similar financial incentives for whistleblowers in the financial services sector. In a note produced jointly with the Prudential Regulation Authority for the Treasury Select Committee, the Financial Conduct Authority (FCA) advised that it would not introduce financial incentives for whistleblowers, having researched the issue (see *FCA: Financial incentives for whistleblowers (July 2014)*). Instead, it planned to press ahead with the regulatory changes necessary to improve whistleblowing procedures within firms, and to make senior management accountable for delivering these procedures. These changes, which came into effect in September 2016, are designed to help create a culture in firms where speaking up becomes the normal business practice, and people are more prepared to report concerns. See *FCA: Whistleblowing*.

LAW COMMISSION REVIEW OF THE SUSPICIOUS ACTIVITY REPORTING REGIME

On 20 July 2018, the Law Commission published a consultation paper on anti-money laundering and the SARs regime (see *Law Commission: Anti-money laundering: the SARs regime: Consultation paper 236 (July 2018)* and *Legal update, Law Commission consultation on the SARS regime*).

Background

The consultation exercise is part of a review being carried out by the Law Commission at the behest of the Home Office. The goal is to improve the prevention, detection and prosecution of money laundering and terrorism financing in the UK by exploring the operation and effectiveness of the existing law around suspicious activity reports (SARs). Alongside its comprehensive and helpful summary of the existing law and guidance (or lack thereof), and some preliminary proposals for reform, the paper seeks responses to 38 consultation questions by the deadline of 5 October 2018.

The paper highlights some striking statistics, including that:

- HMRC has estimated that the annual proceeds of crime in the UK are between £19 billion and £48 billion, with a "best estimate" that approximately £25 billion of money is laundered in the UK every year.
- Money laundering is estimated to cost every household in the UK £255 each year.
- Between 0.7 and 1.28% of the annual Gross Domestic Product of the European Union has been detected to be "involved in suspect financial activity".
- Banks make the vast majority of SARs to the National Crime Agency (NCA) (82.85% between October 2015 and March 2017) with the number rising to 95.78% when including all other types of credit and financial institutions.
- The financial sector in the UK spends at least £5 billion annually on core financial crime compliance, and the cost incurred by a "large reporting bank" in operating an anti-money laundering (AML) program is in the region of "tens of millions of pounds per year".
- On average 2,000 SARs are received by the NCA every working day, with an average of 100 of these seeking consent to proceed with a financial transaction (and thus requiring action within the statutory seven-working-day notice period if the authorities wish to restrain, or at least have an option to restrain, the movement of the relevant funds).
- The NCA has 25 members of staff dedicated to processing this volume of work, but that "all stakeholders" consulted by the Law Commission felt that the system was overburdened and beset by delays.

Key issues identified

A number of practical and legal difficulties with the current system are identified in the paper. In terms of practical problems, the most pressing include this large volume of SARs coupled with the low intelligence value and poor quality of many SARs. The current law appears to drive many of these problems by, amongst other things:

- Casting the net too wide with an "all-crimes" approach (meaning that suspicions of any criminal conduct, no matter how trivial or technical, require the filing of a SAR).
- Incentivising defensive reporting.
- Using imprecise terminology which is often misunderstood and/or inconsistently applied by the reporting sector.
- How the law applies to mixed (criminal and non-criminal) funds.

Other jurisdictions, notably the US and Germany, do not have an "all-crimes" approach in the context of money laundering. Indeed, the UK's "all-crimes" approach exceeds the minimum international standards set by the Financial Action Task Force (FATF) and is not required under European Union law either. While noting that the UK has unnecessarily "gold-plated" its AML regime, and briefly flirting with the idea of proposing a reform to focus on "serious crimes" only, the Law Commission's provisional view is that adopting a "serious crimes" approach could itself create unnecessary complexity and/or be a barrier to successful prosecutions.

However, the paper goes on to seek feedback on three potential alternative "serious crime" approaches (see page 69). In our view, the most promising alternative is to retain the "all-crimes" approach for substantive money laundering offences but only require SARs to be filed in relation to "serious crimes", thus substantially reducing the compliance burden on reporters and removing low value/impact SARs from the system. Another way to address the problem would be to amend the definition of "criminal property" in the Proceeds of Crime Act 2002 (POCA). However, the Law Commission concluded that its terms of reference for this review are too narrow for it to consider this type of change.

The paper also explores the case for defining the concept of "suspicion", which is crucial to the operation of the regime but can be interpreted by different people to "encapsulate a variety of states of mind which exist on a

spectrum from an imagining or inkling to thinking or perhaps believing something to be true or probable." The paper illustrates this variety as ranging from:

- Imagining something without evidence.
- A possibility, which is more than fanciful, that the relevant facts exist.
- Suspicion on some verifiable or articulable grounds.
- Having a strong or settled suspicion that is firmly grounded and targeted on specific facts.

In contrast to other jurisdictions (which require proof of actual "intent" and/or "knowledge" in this context), under English law it need only be proved that a person had a "suspicion" that property may be "criminal property" for that person to be liable for one of the principal money laundering offences in sections 327 to 329 of POCA (provided, of course, that the property in question is in fact "criminal property" and the person carried out one of the acts prohibited by sections 327 to 329). It is again noted in the paper that this ambiguous mental element establishes a much lower threshold than what is envisaged by FATF and the various EU money laundering directives, and has been described as "a remarkably low threshold for a criminal offence", especially one that is punishable by up to 14 years in prison. Despite such criticism, the Law Commission proposes to retain the current threshold of "suspicion" for the purposes of sections 327, 328, 329 and 340 of POCA. However, the paper does raise the prospect of providing a new defence for anyone operating in the regulated sector, as such individuals will regularly encounter criminal property in the course of their work. Accordingly, if such an individual did not have "reasonable grounds" to suspect that property they encountered in their work was "criminal property", then they would not commit one of the section 327 to 329 offences, even if they did have a bare suspicion about the property when they carried out one of the acts prohibited by sections 327 to 329.

One of the most significant and potentially controversial proposals around "suspicion" has more direct relevance to SARs. Under existing law those in the regulated sector must make a disclosure (either to their "nominated officer" or to the NCA if they are the "nominated officer") in circumstances where they know, suspect or have reasonable grounds to suspect, that another person is engaged in money laundering. Any failure to disclose this (without a reasonable excuse) is itself a criminal offence punishable by up to five years in prison. Nominated officers outside the regulated sector are subject to a similar offence.

There is a proposal to remove the mere "suspect" threshold so that the obligation to report would only arise where the person either knows, or has reasonable grounds to suspect, that another person is engaged in money laundering. If enacted, the reform could be accompanied by statutory guidance on how to apply the test.

The proposed reform is a double-edged sword. While it could potentially reduce the scope of the regime and remove defensive or unnecessary SARs from the system, it could paradoxically increase the compliance burden on banks and other reporters (by requiring deeper and more sophisticated analysis of transactions), while also exposing banks and other financial institutions to greater litigation risk. Claimants in this type of litigation have already sought to impose a "reasonableness" test on banks by asserting that while the bank may have been suspicious of a particular transaction, the bank's suspicions were unreasonable and the bank should not have filed a SAR that resulted in a disruption to the operation of the claimant's account and related damages. So far these claims have failed in the courts, but the Law Commission's proposal could give such claimants fresh ammunition if adopted.

Finally, amongst various other proposals, the paper asks for feedback on whether a new corporate "failure to prevent" offence should be created in relation to money laundering. While light on any details, the paper suggests that a commercial organisation could be held criminally liable for its employees' or associates' failure to report suspicions of money laundering or terrorist financing (and/or if the organisation fails to take reasonable measures to ensure that its employees or associates report such suspicions). This type of strict liability corporate offence is obviously modelled on the Bribery Act 2010 and the tax facilitation offence in the Criminal Finances Act 2017. Although not the central focus of the Law Commission's paper, we have our own suspicions that the creation of yet another corporate criminal offence will not be well received by the UK corporate and financial services sector.

Conclusion

The Law Commission's consultation paper is a high-quality survey of current law and practice in this dynamic and topical area. It raises a number of very important questions and proposes a number of helpful and sensible reforms. However, the proposal to remove the mere "suspicion" threshold from the SARs reporting regime may have undesirable side effects that require further consideration.

The consultation paper is just one of a number of important developments in the area of money laundering and the fight against economic crime, including:

- The establishment of a new National Economic Crime Centre within the NCA (see *Legal update, UK economic crime in 2018 and new National Economic Crime Centre*).
- Lisa Osofsky's appointment as the new Director of the Serious Fraud Office (see *Legal update, Lisa Osofsky to be next Director of SFO*).
- The creation and use of new powers, including unexplained wealth orders (see *Practice note, Unexplained wealth orders*).
- The Sanctions and Anti-Money Laundering Act 2018, which is enabling legislation to allow the UK to impose its own economic and other sanctions, and to make provision for money laundering and terrorist financing regulations, after the departure from the EU (see *Practice note, Sanctions and Anti-Money Laundering Act 2018: overview*). It seems unlikely, but is certainly possible, that domestic law will begin to diverge from European law on the subject of AML and sanctions in any post-Brexit environment.
- An increase in the number of money laundering investigations being carried out by the FCA, and frequent comments by Mark Steward (the FCA's Director of Enforcement and Market Oversight) regarding potential criminal prosecutions by the FCA under the Money Laundering Regulations and the FCA's increasing ability to use big data to detect misconduct in the financial markets (see, for example, Mr Steward's recent speech on 3 July 2018 (see *Legal update, FCA speech on action to tackle money laundering in capital markets*)).