April 2019
Volume 10
Number 9

FCPA Update

A Global Anti-Corruption Newsletter

Also in this issue:

If there are additional individuals within your organization who would like to receive *FCPA Update*, please email prohlik@debevoise.com, eogrosz@debevoise.com, or pferenz@debevoise.com

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry

In March, Fresenius Medical Care AG & Co KGaA ("FMC"), a Germany-based medical device and services provider, entered into a long-awaited settlement with the DOJ and SEC, agreeing to pay more than $231 million to resolve allegations that FMC and its subsidiaries paid bribes to government officials and healthcare professionals employed by public health systems in multiple countries in order to grow business and facilitate the opening of new medical centers around the world. According to the settlement papers, senior management and the FMC Board were aware of and involved in some of the misconduct. The $231 million settlement is second only to the Teva case as the largest FCPA settlement brought in the life sciences area. FMC also agreed to the imposition of an independent monitor for a two-year period, because enhancements to its compliance program were relatively new and untested as of the time of the settlements.

Continued on page 2

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry
Continued from page 1

There are a few noteworthy aspects to the settlement.

First, in addition to agreeing to pay $147 million in disgorgement and pre-judgment interest to the SEC,[1] the company also agreed to pay a criminal penalty of $84 million,[2] which represented a 40% discount off the bottom end of the U.S. Sentencing Guidelines range.[3] Although it is not entirely clear from the DOJ papers why the company received a 40% discount, it appears to have been driven in large part by the fact that FMC self-reported some of the improper payments to DOJ and the SEC in 2012, but did not fully cooperate.[4] Both agencies noted that FMC's cooperation varied over time, and for that reason, neither agency gave the company full cooperation credit.[5] Presumably, given the extent of the conduct, the amount of the profit, and the fact that employees at the parent issuer were implicated, it was unlikely that FMC would have qualified for a declination under DOJ's Corporate Enforcement Policy.

Second, as discussed below, the breadth of the conduct was extensive. DOJ and SEC alleged conduct in seventeen different countries, including eight countries in "West Africa," Angola, Morocco, Saudi Arabia, Turkey, Bosnia, Serbia, China, and Mexico. Interestingly, the SEC alleged violations of the anti-bribery provisions in ten countries (Angola, Saudi Arabia and the eight countries in West Africa), while DOJ only brought bribe charges in two (Angola and Saudi Arabia). This may be a result of the agencies' respective view of the strength of the evidence relating to the use of interstate commerce, as discussed below.

Finally, the FMC settlement demonstrates the difficulties that a large multinational company can have when it chooses to self-report. In this case, it appears clear that FMC did not know the full extent of the conduct when it made the initial self-report in 2012. Given the length of time it took to resolve the matter after the initial self-report in 2012, it may be that the U.S. authorities were frustrated by the amount of time it took to fully investigate the company's conduct.

Continued on page 3

1. Order, *In re Fresenius Medical Care AG & Co. KGaA*, Securities Exchange Act Rel. No. 85468 §§ IV(A), (B), (C) (Mar. 29, 2019), https://www.sec.gov/litigation/admin/2019/34-85468.pdf [hereinafter "SEC Order"].
2. Letter from the U.S. Dep't of Justice to Maxwell Carr-Howard Re: *Fresenius Medical Care AG & Co. KGaA*, 6 (Feb. 25, 2019), https://www.justice.gov/opa/press-release/file/1148951/download [hereinafter "DOJ NPA"].
3. *Id*. at 6.
4. *See* SEC Order ¶ 62 (stating that FMC self-reported "certain misconduct").
5. For example, the DOJ NPA states that FMC did not always respond to DOJ's requests in a timely manner and occasionally did not provide "fulsome" responses to DOJ's information requests. FMC NPA at 1-2.

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry
Continued from page 2

FMC's FCPA Violations

FMC admitted that, between 2007 and 2016, certain of its foreign subsidiaries made almost $30 million in improper payments to government officials.[6] FMC's operations span 150 countries[7] and the misconduct cited in the FMC Order and FMC NPA covered conduct involving 17 of them.[8] As is common with cases in the life sciences area, the alleged wrongdoing includes a variety of conduct: larger payments to healthcare professionals,[9] smaller payments to healthcare providers[10] and customs officials,[11] and the ubiquitous generalized allegations of improper gifts, meals, entertainment, and travel.[12] Payments were made in cash,[13] through third parties,[14] and via investment and employment opportunities.[15] Some of the payments involved senior management and even members of FMC's Board.[16] Others were made by local employees or management in contravention of directives from their supervisors.[17]

"[I]t appears clear that FMC did not know the full extent of the conduct when it made the initial self-report in 2012…. Any expansion of the investigation undoubtedly increased both investigative costs and the final profit-driven penalty calculation. This highlights the importance of understanding, as much as possible, the scope of the potential problems at the time of self-reporting."

Though the wide-ranging conduct spanned 17 jurisdictions, DOJ only brought bribery charges in two countries (Saudi Arabia and Angola), whereas the SEC found violations of the anti-bribery provisions in 10 countries (Saudi Arabia, Angola, and 8 West African countries). This likely stems from the agencies' differing views of

Continued on page 4

6. SEC Press Release No. 2019-48, *SEC Charges Medical Device Company With FCPA Violations* (Mar. 29, 2019), https://www.sec.gov/news/press-release/2019-48 [hereinafter "SEC Press Release"].
7. FMC Order ¶ 2.
8. The FMC Order lists 16 countries in one paragraph (FMC Order ¶ 2) and adds Morocco later in the Order (FMC Order ¶ 5).
9. FMC Order ¶¶ 6-8, 13-16, 19, 26-29, 34-41, 43-47, 53-54; FMC NPA Attachment A ¶¶ 16-23, 27-28, 38-47, 57-63, 74-77, 79-80, 89-96, 104-111.
10. FMC Order ¶¶ 55-57.
11. FMC NPA Attachment A ¶¶ 48.
12. FMC NPA Attachment A ¶¶ 45-47, 78.
13. FMC Order ¶ 10.
14. FMC Order ¶¶ 13-15.
15. FMC NPA Appendix A ¶¶ 89-96.
16. FMC Order ¶¶ 38, 40.
17. FMC Order ¶¶ 32-33.

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry
Continued from page 3

the evidence supporting the requisite interstate commerce element. To find FMC, a foreign issuer, liable for anti-bribery violations, the U.S. enforcement agencies have to establish that FMC "ma[d]e use of the mails or any means or instrumentality of interstate commerce."[18] As in other cases, DOJ and the SEC rely on "internet-based email accounts hosted by numerous service providers located in the United States."[19] Although it may seem a thin reed, at least one court has held that use of a U.S.-based internet server can be sufficient, even if the participants are not aware that their email will bounce on a U.S. server.[20]

The DOJ NPA and the SEC Order also found that FMC failed to implement reasonable internal controls and to maintain accurate books and records in all 17 countries in which the SEC found misconduct, including China, Serbia, Bosnia, Mexico, and eight countries in West Africa.[21] Among other things, FMC acknowledged that senior management had directed employees to destroy records of the misconduct and that FMC had not provided anti-corruption training or performed due diligence on its agents.[22]

According to the resolutions, FMC generated a profit of approximately $140 million from the bribes over a nine-year period.[23] Notably, the SEC made no mention of the statute of limitations requirements arising from the *Kokesh*[24] decision, possibly because the company had agreed to toll the statute of limitations.

Key Takeaways

- **DOJ and SEC continue to focus on the life sciences industry.** As has been noted in previous issues of *FCPA Update*, the SEC and DOJ continue to focus on life sciences companies.[25] FMC provides a useful reminder that even small payments in multiple jurisdictions can be aggregated to form the basis for large fine and disgorgement amounts.

Continued on page 5

18. 15 U.S.C §78dd-1(a).
19. FMC Order ¶ 1 ("In connection with the misconduct described in Saudi Arabia, West Africa, and Angola, FMC employees and agents utilized the means and instrumentalities of U.S. interstate commerce, including the use of internet-based email accounts hosted by numerous service providers located in the United States"), FMC NPA, Attachment A ¶ 5 ("In Angola and Saudi Arabia, these agents and employees utilized the means and instrumentalities of U.S. interstate commerce, including the use of internet-based email accounts hosted by numerous service providers located in the United States.").
20. SEC v. Straub, 921 F. Supp. 2d 244, 255–56 (S.D.N.Y. 2013).
21. SEC Press Release at 1; FMC Order ¶ 60.
22. SEC Press Release at 1.
23. DOJ Press Release No. 19-290, *Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges* at 1 (Mar. 29, 2019), https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve.
24. Kokesh v. SEC, 137 S. Ct. 1635 (2017).
25. *See* Kara Brockmeyer, Andrew M. Levine, Paul D. Rubin, Philip Rohlik, & Andreas A. Glimenakis, *Sanofi Settlement Highlights Risk in the Life Sciences Industries*, FCPA Update, Vol. 10, No. 2 (Sept. 2018) https://www.debevoise.com/~/media/files/insights/publications/2018/09/20180928_fcpa_update_september_2018_v2.pdf.

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry
Continued from page 4

- **DOJ and the SEC continue to promote voluntary self-disclosure by offering significant benefits.** Even though FMC self-reported in 2012 – three years before the Yates Memorandum and five years before the Corporate Enforcement Policy – it reaped at least some of the Policy's self-reporting benefits. Despite senior management involvement in certain schemes (and Board knowledge of others[26]) and the fact that the misconduct appears to have continued for years after the initial self-report, FMC received a 40% discount off the bottom of the U.S. Sentencing Guidelines range. That underscores the potential value of self-reporting misconduct.
- **However, there are hazards to self-reporting.** Despite the significantly discounted fine, FMC's total penalty amount is large compared to other life sciences cases.[27] FMC did not publicly disclose which countries were involved in its initial self-report,[28] but it seems likely that FMC's investigation expanded afterwards. That would explain the number of jurisdictions involved, the fact that misconduct in some jurisdictions continued until 2016, and the credit received for "disclosing conduct to the Department that was outside the scope of its initial voluntary self-disclosure."[29] Any expansion of the investigation undoubtedly increased both investigative costs and the final profit-driven penalty calculation.[30] This highlights the importance of understanding, as much as possible, the scope of the potential problems at the time of self-reporting.
- **Appropriate compliance staffing is important.** The FMC Order calls out FMC's failure to appoint a compliance officer for the region that included Saudi Arabia in connection with conduct occurring prior to 2012.[31] While this can be viewed as an example of the SEC's application of today's best practices to the past, companies have been on notice of the need to appropriately staff regional

Continued on page 6

26. FMC Order ¶¶ 38, 40.
27. For example, in 2018 Sanofi paid about $25 million to settle FCPA violations (SEC Press Release No. 2018-174, *Sanofi Charged with FCPA Violations* (Sept. 4, 2018), https://www.sec.gov/news/press-release/2018-174) and in 2017 Orthofix paid over $14 million (SEC Press Release No. 2017-18, *Medical Device Company Charged with Accounting Failures and FCPA Violations* (Jan. 18, 2017), https://www.sec.gov/news/pressrelease/2017-18.html). The only life sciences company that has paid more than FMC to settle FCPA violation is Teva, which paid a total of more than $540 million in 2016. Office of Public Affairs, *Teva Pharmaceutical Industries Ltd. Agrees to Pay More Than $283 Million to Resolve Foreign Corrupt Practices Act Charges*, Dep't of Justice Press Release No. 16-1522, 1 (Dec. 22, 2016), https://www.justice.gov/opa/pr/teva-pharmaceutical-industries-ltd-agrees-pay-more-283-million-resolve-foreign-corrupt.
28. FMC's 2013, 2014, and 2015 20-F filings disclose that FMC "received communications alleging certain conduct in certain countries outside the US and Germany" that might violate anti-bribery laws, including the FCPA. FMC's 2016, 2017, and 2018 20-F filings acknowledge the investigations and FMC's cooperation efforts and remedial actions.
29. FMC NPA at 1.
30. The potential unfairness of increasing fines and disgorgement as the result of investigative steps that likely would not have been taken but for a company's self-reporting is an area that merits consideration by the enforcement agencies.
31. FMC Order ¶ 6.

Fresenius Settlement Demonstrates Continued Regulatory Interest in Life Sciences Industry

Continued from page 5

compliance positions since at least the Bristol-Myers Squibb enforcement action in 2015.[32] Companies must ensure that compliance programs and internal controls "keep up" as the business expands.[33]

- **It is important to quickly respond to red flags.** As in other cases,[34] the SEC noted that FMC was slow to respond to potential issues as they arose. The SEC faulted FMC for taking eight months after a whistleblower report to start an internal investigation in Morocco[35] and five months to undertake a legal and compliance review of a contract identified as problematic in Angola.[36]
- **DOJ and the SEC continue to assert aggressive jurisdictional theories**, as demonstrated by their stated use of only U.S.-hosted email accounts to establish a jurisdictional nexus.

Jane Shvets

Philip Rohlik

Jil Simon

Andreas A. Glimenakis

Katherine L. Nelson

Jane Shvets is a partner in the London office. Philip Rohlik is a counsel in the Shanghai office. Jil Simon, Andreas A. Glimenakis, and Katherine L. Nelson are associates in the Washington, D.C. office. The authors may be reached at jshvets@debevoise.com, prohlik@debevoise.com, jsimon@debevoise.com, aaglimen@debevoise.com, and klnelson@debevoise.com. Full contact details for each author are available at www.debevoise.com.

Continued on page 7

32. Order, *In re Bristol-Myers Squibb Company* ¶ 9, Securities Exchange Act Rel. No. 76073 (Oct. 5, 2015), https://www.sec.gov/litigation/admin/2015/34-76073.pdf.
33. SEC Press Release at 1 ("[f]ailure to address the corruption risks in its growing business allowed complicit managers to engage in bribery schemes that went undetected for more than a decade."); U.S. Dep't of Justice, *Assistant Attorney General Brian A. Benczkowski Delivers Remarks at the 33rd Annual ABA National Institute on White Collar Crime Conference*, 1 (Mar. 8, 2019), https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-33rd-annual-aba-national; *see also* Andrew M. Levine, Philip Rohlik, & Kamya B. Mehta, *Mitigating Anti-Corruption Risk in M&A Transactions: Successor Liability and Beyond*, FCPA Update, Vol. 10, No. 5 (Dec. 2018) https://www.debevoise.com/~/media/files/insights/publications/2018/12/201812_fcpa_update_december_2018.pdf.
34. *See* Andrew M. Levine, Jane Shvets, Colby A. Smith, Philip Rohlik, & Olivia Cheng, *FCPA Settlements Reached with Beam Suntory and Credit Suisse*, FCPA Update, Vol. 9, No. 12 (July 2018), https://www.debevoise.com/~/media/files/insights/publications/2018/07/fcpa_update_july_2018_v3.pdf.
35. FMC Order ¶ 17.
36. FMC Order ¶ 33.

U.K. Legislator Clears the Way for Extraterritorial Production Orders

Overview of the COPOA Regime[1]

Electronic data, often essential to the effective investigation and prosecution of serious international criminality, is frequently located overseas. This data is typically obtained through Mutual Legal Assistance ("MLA") treaties, but these procedures are generally protracted and cumbersome, and often result in delayed or even abandoned pursuits of evidence. Letters of request for mutual assistance can take up to two years to process, primarily because MLA entails a state-to-state, bureaucratic procedure, requiring approval by the requested country's judicial authorities. Time delays of this nature are clearly inadequate when investigating live conspiracies with immediate risks of further harm, or when prosecuting cases where the harm caused has lasting effects.

In an attempt to address some of the difficulties in the MLA process, a new legislative framework received Royal Assent in the U.K. on February 12, 2019. The Crime (Overseas Production Orders) Act 2019 ("COPOA") aims to simplify and accelerate the obtaining by criminal investigators of electronic data located abroad. It provides for a court-issued Overseas Production Order ("OPO") to compel persons located overseas, particularly Communication Services Providers ("CSPs"), to produce or grant access to electronic data. OPOs will be capable of compelling companies directly, without involvement from the authorities in the target jurisdiction. The person subject to an OPO must operate or be based outside the U.K., and be in a country that is party to a "designated international cooperation arrangement."[2] This is essentially a treaty which relates to the provision of mutual assistance in connection with the investigation or prosecution of offences, and specifically designated for the purposes of COPOA. No such treaty currently exists, but negotiations are underway with the United States – home to Facebook, Google, and other CSPs hosting vast sources of electronic data – for a treaty that will serve as a "framework for other reciprocal treaties all around the world."[3]

Parliament has not yet announced when the COPOA regime will come into force – but if the legislative objectives are realised, it will serve as a powerful tool in transnational evidence gathering.

Continued on page 8

1. This is a slightly expanded version of an article first published in the May 2019 issue of PLC Magazine, *see* http://uk.practicallaw.com/resources/uk-publications/plc-magazine.
2. Section 4(2) COPOA.
3. Nick Thomas-Symonds MP speaking in a parliamentary debate on COPOA on January 30, 2019 (https://hansard.parliament.uk/Commons/2019-01-30/debates/F3A6039F-B824-4EDB-AB6F-54C1932F3E36/Crime(OverseasProductionOrders)Bill(Lords)).

U.K. Legislator Clears the Way for Extraterritorial Production Orders
Continued from page 7

Operation of the COPOA Regime

In order to obtain electronic data pursuant to the COPOA regime, an "appropriate officer" will have to make an *ex parte* application to the Crown Court for an OPO requiring the production of specified electronic data.[4] Persons able to apply for an OPO comprise a wide range of investigating authorities, including police constables, HMRC officers, members of the Serious Fraud Office, and individuals appointed by the Financial Conduct Authority.[5]

Electronic data is defined widely, involving "any data stored electronically".[6] It therefore encompasses many categories of electronic data, including everything from emails and electronic documents to pictures and videos. Data protected by legal professional privilege, as well as confidential personal records relating to physical or mental health, or to counselling related to spirituality or personal welfare, cannot be sought by means of an OPO.[7]

The Crown Court Judge will apply a six-part test to assess an OPO application,[8] and must be satisfied that there are reasonable grounds for believing that:

1. The person against whom the order is sought operates or is based outside the U.K. in a country that is party to, or participates in, a specified designated international cooperation agreement;
2. Either an indictable offence has been committed and is being investigated or proceedings in respect of the offence have been instituted, or the OPO is sought for the purposes of a terrorist investigation;
3. The person against whom the order is sought has possession or control of all or part of the electronic data specified or described in the application for the OPO;
4. All or part of the electronic data specified or described in the application for the order is likely to be of substantial value (by itself or in context) to the proceedings or investigation;
5. All or part of the electronic data is likely to be relevant evidence, and admissible in proceedings in respect of the relevant offence;[9] and
6. It is in the public interest for all or part of the data to be produced. Relevant considerations include the benefit likely to accrue to the proceedings or investigations if the data is obtained.

Continued on page 9

4. Section 1(1) COPOA.
5. Section 2(1) COPOA.
6. Section 3(2) COPOA.
7. Section 3(3) COPOA.
8. Section 4 COPOA.
9. This provision does not apply to terrorism investigations.

U.K. Legislator Clears the Way for Extraterritorial Production Orders
Continued from page 8

If these conditions are satisfied, the Judge *may* approve the OPO. An OPO will set out: the electronic data requested; the person (or description of the person) to whom the electronic data must be produced or granted access to; and the date by which the OPO must be complied with.[10] An OPO must ordinarily be complied with within seven days, but the Judge has discretion to specify an alternative time frame where necessary.[11]

Once approved, the OPO may only be served on the overseas person by the Secretary of State (for orders made in England, Wales, or Northern Ireland) or Lord Advocate (for orders made in Scotland), who must as a prerequisite determine that such service is in accordance with the relevant designated international cooperation arrangement.[12] Such service can be effected on the overseas person at its principal place of business in the U.K.[13]

"[COPOA] aims to simplify and accelerate the obtaining by criminal investigators of electronic data located abroad. It provides for a court-issued Overseas Production Order … to compel persons located overseas, particularly Communications Services Providers…, to produce or grant access to electronic data."

Impact on Persons Subject to OPOs

Persons subject to an OPO are compelled to produce or grant access to electronic data that they possess or control, wherever that data may be located. During this period, the person must not conceal, destroy, alter, or otherwise dispose of any of the electronic data specified or described in the OPO. However, the requirement to produce or give access to electronic data does not require the person to do anything that would result in a contravention of data protection legislation.[14] The person may also be subject to a strict duty of confidentiality, and must not disclose the making of the application or its contents to any person, including those directly affected by the order.[15] Any person affected by an OPO may apply to a Crown Court Judge to vary or revoke it.[16]

Continued on page 10

10. Section 5 COPOA.
11. Section 5(5) COPOA.
12. Section 9(4) COPOA.
13. Sections 9 and 14(3)(a) COPOA.
14. Section 6(4)(c) COPOA.
15. Section 8 COPOA.
16. Section 7(2)(b) COPOA.

The scope of the COPOA regime and the potential application of OPOs is wide. Although Parliamentary debate principally focused on CSPs as the primary recipients of OPOs, particularly in relation to sex offences and terrorism prevention, their applicability is universal and OPAs will likely be increasingly deployed in white collar enforcement.

One of the weaknesses of COPOA is the relatively ineffective sanctions framework for persons who fail to comply with an OPO. Those who fail to comply may be held in contempt of court in the U.K., with penalties including fines and imprisonment. In practice, however, this has limited effect internationally not least because contempt of court is currently not an extraditable offence. Nevertheless, failure to comply can carry strong reputational consequences, which CSPs are likely to want to avoid.

The most significant limitation, however, is that court powers to approve an OPO will only be exercisable where a relevant international cooperation arrangement exists between the U.K. and the target jurisdiction. As already pointed out, there are as yet no international agreements to attach it to. The expected reciprocal treaty with the United States was envisaged by the U.S. Clarifying Lawful Overseas Use of Data Act 2018 ("the CLOUD Act"), which authorises the U.S. government to form bilateral agreements with other governments to facilitate cross-boarder electronic data access.

Treaties with other jurisdictions may follow, particularly if the U.K. loses access to the European Investigation Order ("EIO") regime as a consequence of Brexit. CSPs operating or based in the U.K. would therefore be well-advised to review the corresponding legislation in countries with which the U.K. concludes designated international agreements.

Interaction with SFO Section 2 Notices Following *KBR*

Currently, the SFO can compel an individual or entity to produce "documents", which includes electronic material, believed to be relevant to a matter under investigation by issuing notices under section 2(3) of the Criminal Justice Act 1987 (so-called "Section 2 notices"). In September 2018 the High Court ruled in *R (On the Application of KBR Inc) v The Director of the Serious Fraud Office*[17] that Section 2 notices had extraterritorial effect in so far as they could be served on foreign companies with respect to documents held outside the jurisdiction where there is a "*sufficient connection*" between the company and the U.K.

Continued on page 11

17. [2018] EWHC 2368 (Admin).

U.K. Legislator Clears the Way for Extraterritorial Production Orders
Continued from page 10

For companies subject to an SFO investigation, therefore, the advent of the OPO is likely to make very little difference in practice; if the SFO claims jurisdiction to prosecute, there is very likely to be a sufficient connection between the suspect company and the U.K. The SFO can therefore continue to require from companies under investigation that they produce electronic material stored abroad by means of Section 2 notices.

OPOs are however likely to make a material difference to SFO investigations in two main circumstances: First, obtaining data from non-suspect persons and entities outside the U.K. believed to have information relevant to an investigation, since it will be possible to issue OPOs to persons and entities irrespective of their connection to the U.K. Second, in relation to material located in jurisdictions where blocking statutes or other legislation preventing the export of data can only be overridden by request based on an international treaty, since OPOs will be premised on a designated cooperation arrangement.

COPOA: Part of an International Trend

The enactment of COPOA is part of a wider movement towards speeding up the gathering of evidence in international criminal investigations, and marks a departure from the current MLA process. With its strict time limits, OPOs should enable appropriate officers to obtain vital evidence within weeks, if not days.

Indeed, ministers and law enforcement officials have hailed OPOs as a swift and welcome alternative to MLA. Assistant Chief Constable Richard Berry[18] stated: "The cumbersome nature of long-standing arrangements for mutual legal assistance has for many years inhibited the speed at which U.K. policing has been able to access vital information stored in other countries. More timely access to such data is welcome, and the provisions in [the Act] can speed up investigations whilst still allowing for in-built judicial safeguards and scrutiny."[19]

Additionally, COPA also reflects an international trend in simplifying electronic data evidence gathering. On April 17, 2018, the European Commission produced a draft European Regulation which would provide for the production and preservation of electronic evidence in intra-EU criminal investigations and prosecutions. This "European Production Order" ("EPO") is intended to enable judicial authorities in one Member State to easily obtain electronic data (such as emails, texts or messages received through smartphone applications) directly from a service provider or its

Continued on page 12

18. The National Police Chiefs' Council lead for Communications Data.

19. "Crime (Overseas Production Orders) Bill Receives Royal Assent" (Feb. 12, 2019), https://www.gov.uk/government/news/crime-overseas-production-orders-bill-receives-royal-assent?utm_source=97b15479-d7eb-4f1b-ae2e-3c6e8b9d0bc4&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate.

U.K. Legislator Clears the Way for Extraterritorial Production Orders
Continued from page 11

legal representative in another Member State. The subject of the order will then have ten days, or six hours in cases of emergency, to respond. This is also a vast improvement from the current timeframe of up to 120 days under the existing European Investigation Order regime. To support this process, judicial authorities will also be empowered to issue European Preservation Orders to preserve electronic evidence data in view of subsequent production orders.

More recently, on February 5, 2019, a week before COPOA received Royal Assent, the European Commission submitted a recommendation to the European Council to commence international negotiations on behalf of the European Union on cross-border access to electronic evidence. The Commission presented two negotiating directives. The former detailed relevant negotiations with the United States. The latter concerned the Second Additional Protocol to the Council of Europe "Budapest" Convention on Cybercrime: a multilateral treaty that provides a legal framework for the fight against crimes committed over the internet and other computer networks. Changes to be introduced by the Second Additional Protocol will focus on four key elements: (1) measures to improve international cooperation between law enforcement and judicial authorities, including on mutual legal assistance; (2) cooperation between authorities and service providers in other countries; (3) conditions and safeguards for access to information by authorities in other countries; and (4) other safeguards, including data protection requirements. Negotiations on the protocol are expected to conclude by December 2019.

In short, it seems that the COPOA regime is in line with the changing international approach to gathering e-evidence from other jurisdictions: quicker, simpler, and based on reciprocity.

Karolos Seeger

Robin Lööf

Ramsay McCulloch

Aisling Cowell

Karolos Seeger is a partner in the London office. Robin Lööf is an international counsel in the London office. Ramsay McCulloch and Aisling Cowell are associates in the London office. The authors may be reached at kseeger@debevoise.com, rloof@debevoise.com, rmcculloch@debevoise.com, and acowell@debevoise.com. Full contact details for each author are available at www.debevoise.com.

FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

London
+44 20 7786 9000

Paris
+33 1 40 73 12 12

Frankfurt
+49 69 2097 5000

Moscow
+7 495 956 3858

Hong Kong
+852 2160 9800

Shanghai
+86 21 5047 1800

Tokyo
+81 3 4570 6680

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Andrew J. Ceresney
Co-Editor-in-Chief
+1 212 909 6947
aceresney@debevoise.com

David A. O'Neil
Co-Editor-in-Chief
+1 202 383 8040
daoneil@debevoise.com

Jane Shvets
Co-Editor-in-Chief
+44 20 7786 9163
jshvets@debevoise.com

Philip Rohlik
Co-Executive Editor
+852 2160 9856
prohlik@debevoise.com

Andreas A. Glimenakis
Associate Editor
+1 202 383 8138
aaglimen@debevoise.com

Kara Brockmeyer
Co-Editor-in-Chief
+1 202 383 8120
kbrockmeyer@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Karolos Seeger
Co-Editor-in-Chief
+44 20 7786 9042
kseeger@debevoise.com

Erich O. Grosz
Co-Executive Editor
+1 212 909 6808
eogrosz@debevoise.com

Jil Simon
Associate Editor
+1 202 383 8227
jsimon@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

Please note:
The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.