LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Why Ericsson DPA Breach Is Precedent-Setting

By **James Koukios and Sarah Maneval** (May 25, 2023, 4:17 PM EDT)


James Koukios


Sarah Maneval

On March 2, the U.S. Department of Justice announced that Sweden-based telecommunications company Telefonaktiebolaget LM Ericsson had agreed to plead guilty to Foreign Corrupt Practices Act violations and pay over $200 million for breaching its 2019 deferred prosecution agreement involving alleged bribery schemes and other misconduct in Asia, Africa and the Middle East.[1]

According to the DOJ, the company violated the DPA's cooperation and disclosure provisions by failing to truthfully disclose all factual information and evidence related to three alleged bribery schemes in Djibouti, China and Iraq.

Breaches of DPAs are rare and, when they do occur, are typically the result of something that has happened after the DPA was entered, such as new or continuing misconduct, or a failure to implement an agreed remedial measure.

The Ericsson breach suggests that the DOJ may also look backward to declare a breach based on deficient preresolution disclosures — a sobering standard for companies and their counsel contemplating a resolution with the DOJ.

Ericsson's Breach of the Deferred Prosecution Agreement

In December 2019, the DOJ and the U.S. Securities and Exchange Commission announced that Ericsson had agreed to pay a total of approximately $1.06 billion to resolve FCPA allegations involving alleged bribery schemes in China, Djibouti, Indonesia, Kuwait, Saudi Arabia and Vietnam.

The alleged misconduct included, among other things, the improper use and retention of third parties, gifts, travel and entertainment, and the procurement of inside information about a government tender.

The Swedish parent company entered into a three-year DPA, filed in the U.S. District Court for the Southern District of New York, under which it agreed to pay a criminal penalty of over $520 million and accept an independent compliance monitor.

A subsidiary, Ericsson Egypt Ltd., pled guilty to criminal charges in the Southern District of New York.

In calculating the criminal penalty, the DOJ stated that the company did not receive full credit for cooperation and remediation under the FCPA corporate enforcement policy because, among other

things, it did not disclose allegations of corruption with respect to two matters and produced certain materials in an untimely manner.

The criminal penalty reflected a 15% discount off the low end of the U.S. sentencing guidelines range, instead of the 25% discount that would have been available for full cooperation and remediation.

Separately, the parent company resolved the SEC's civil charges by agreeing to pay about $540 million in disgorgement and prejudgment interest.

The combined resolution was, and remains, the largest U.S.-only resolution in the history of FCPA enforcement.

Like all FCPA-related DPAs, the Ericsson DPA required the company to "truthfully disclose all factual information with respect to its activities," provide "any document, record, or other tangible evidence about which [the DOJ] may inquire of the Company," and promptly report any evidence that an FCPA violation may have occurred — the cooperation and disclosure requirements — during the term of the DPA.

As is usual, the DPA also stated that if the company provided deliberately false, incomplete or misleading information, or failed to comply with the cooperation and disclosure requirements, then the DOJ could declare a breach and prosecute the company for any federal criminal violation of law, including but not limited to the charges set out in the information that accompanied the DPA.

Alternatively, the DOJ could extend the term of the DPA up to one year.

On March 2, the DOJ announced that Ericsson had breached the DPA and had agreed to plead guilty to the two charges originally deferred by the DPA: conspiracy to violate the FCPA's anti-bribery provisions and conspiracy to violate the FCPA's accounting provisions.

In addition to an earlier agreement to extend its independent compliance monitor by one year, the company also agreed to pay an additional fine of approximately $207 million, which is the difference between the midpoint of the U.S. sentencing guidelines range for the offense conduct set out in the DPA and the amount that the company already paid pursuant to the DPA.

According to the DOJ, Ericsson violated the DPA's cooperation and disclosure requirements in two ways.

First, the DOJ alleged that Ericsson failed to provide it with all the evidence the company had identified regarding the Djibouti and China bribery schemes underlying the DPA, which "prevented the United States from bringing charges against certain individuals and taking key investigative steps."[2]

In particular, the DOJ alleged that Ericsson had failed to produce an email suggesting that two Ericsson executives were aware of the Djibouti scheme; an email from an Ericsson manager alleging that certain Ericsson executives had engaged in improper relationships with third-party agents central to the China scheme; and hard-copy documents relevant to the China scheme.

Second, the DOJ alleged that Ericsson had failed to provide information regarding potential misconduct in Iraq.

According to the DOJ, two weeks before entering into the DPA, the company "disclosed generalized

information ... relating to a new internal investigation it was conducting concerning" Iraq. This disclosure, however, "omitted key details, ... material facts and information, ... [and] evidence of possible misconduct that were known to the Company and its prior outside counsel" at the time.

The company finalized the Iraq investigation just five days after the DPA was entered, but did not disclose the findings until February 2022, after the company was contacted by an investigative journalist.

Breaches of Deferred Prosecution Agreements

DPAs have become a common means of resolving corporate criminal cases, particularly in FCPA cases.

According to the Organization for Economic Cooperation and Development's Working Group on Bribery, which monitors U.S. compliance with the OECD Anti-Bribery Convention, between September 2010 and July 2019, the DOJ used DPAs in 41%, and nonprosecution agreements in 23%, of its concluded FCPA corporate enforcement actions involving legal persons.[3]

Despite the prevalence of DPAs, breaches of DPAs are relatively rare. In 2019, for example, it was reported that DOJ had entered into more than 500 DPAs and NPAs since 2000, but only about a dozen had resulted in breaches.[4]

The DOJ has found breaches of only a handful of FCPA-related DPAs. When the DOJ is concerned about a company's compliance with the terms of a DPA, it typically extends the term of the DPA.

In U.S. v. Orthofix International NV, for example, the DOJ extended the term of the DPA, entered in July 2012, for two months after reports surfaced post-resolution that the company's Brazilian subsidiary may have made improper payments to doctors at government-owned hospitals.[5]

In U.S. v. Bilfinger SE, the DOJ extended the DPA, entered in December 2013, for two years after the independent compliance monitor concluded that the company had not fulfilled the DPA's enhanced compliance requirements.[6]

And in U.S. v. Mobile Telesystems PJSC, the DOJ extended the DPA, entered in February 2019, for one year because it determined that the company had not yet effectively implemented and tested all components of its enhanced compliance program.[7]

In some cases, the DOJ has imposed more severe penalties for violations of DPAs.

Aibel Group Ltd., for example, pled guilty to FCPA violations and agreed to pay $4.2 million in criminal penalties as well as submit to a two-year term of organizational probation after the company admitted that it was not in compliance with a DPA entered the prior year.[8]

In another example, the DOJ required Zimmer Biomet Holdings Inc. to pay $17.4 million in criminal penalties and enter into a new DPA because the company allegedly committed additional FCPA violations after entering into the first DPA and failed to implement an enhanced compliance program.[9]

Importantly, all of the cases described above involved post-resolution conduct — either new or continuing misconduct, or a failure to implement enhanced compliance measures.

Although Ericsson technically had a continuing duty to provide the DOJ with evidence post-resolution, the gravamen of the breach was the failure to provide complete information to the DOJ preresolution. Thus, the Ericsson case sets a new precedent for when the DOJ will declare a breach.

Takeaways

With the caveat that resolutions do not always reveal the precise reasons for the DOJ's charging decisions, there are several potential practice takeaways from the Ericsson breach.

First, the DOJ seems to have concluded that Ericsson intentionally withheld damaging documents related to China and Djibouti before entering into the DPA.

But in some cases, inculpatory documents can be innocently missed when companies reasonably focus on documents from certain jurisdictions, time periods or data sources, or those written in certain languages, in response to data privacy concerns, technological challenges or a desire to maximize investigative resources.

Being abundantly clear with the DOJ about the review and production parameters used in an investigation could help a company avoid creating a perception that later-discovered documents had been strategically withheld.

Second, the DOJ seemed particularly concerned that Ericsson had mischaracterized or downplayed the Iraq allegations.

Although it is important to efficiently convey to the DOJ information learned from an investigation or contained in a whistleblower report, the disclosures must not be misleading.

Before making any disclosure, companies should take a step back and consider whether the DOJ might perceive that the company has omitted details or minimized the seriousness of any potential misconduct.

It is particularly important not to downplay the seriousness of late-breaking allegations simply to get the deal done.

Even with relatively serious allegations, the DOJ may be content to finalize the deal and allow the company to report on the results of the investigation and any related remediation during the DPA's reporting period.

Third, and relatedly, companies should be prepared to revisit past disclosures if new information emerges that could be seen as casting new light on those disclosures. This is perhaps the most challenging — and most sobering — of the potential lessons from the Ericsson breach.

It is not unusual for companies to disclose additional allegations and investigative findings to the DOJ during the pendency of an investigation or during the DPA's reporting period.

The Ericsson breach does not mean that companies must constantly revisit these disclosures. But if new information comes to light that calls into question the accuracy of a prior representation, then companies should consider amending the record.

Being proactive in these situations can help the company put the new information in proper context and reassure the DOJ that the company is committed to transparency and remediation, which can help avoid a perception that the company has breached the DPA.

Although DPA breaches remain rare, the Ericsson case is a concrete example of the DOJ following through on Deputy Attorney General Lisa Monaco's October 2021 promise that DOJ "will hold accountable any company that breaches the terms of its DPA or NPA."[10]

This might be a signal of greater scrutiny of companies who have entered, or have contemplated entering, a DPA with the DOJ.

James Koukios is a partner, co-chair of the securities litigation, enforcement and white collar defense group, and co-head of the FCPA and global anti-corruption practice at Morrison Foerster LLP.

Sarah Maneval is an associate at the firm.

[1] Ericsson, Deferred Prosecution Agreement (Apr. 20, 2023), available at https://www.justice.gov/criminal-fraud/file/1576986/download.

[2] Press Release, Dep't of Justice, Ericsson to Plead Guilty and Pay Over $206M Following Breach of 2019 FCPA Deferred Prosecution Agreement (Mar. 2, 2023), available at https://www.justice.gov/opa/pr/ericsson-plead-guilty-and-pay-over-206m-following-breach-2019-fcpa-deferred-prosecution.

[3] See OECD Working Group on Bribery, United States Phase 4 Report (Oct. 16, 2020), at 51.

[4] Sue Reisinger, "Three Companies Learn the Hard Way: Don't Breach a Federal Non-Prosecution Agreement," Law.com (Mar. 4, 2019).

[5] Orthofix also agreed to pay more than $14 million to resolve these allegations with the SEC. Joint Status Report, U.S. v. Orthofix Int'l N.V., No. 4:12-CR-00150-RAS-DDB-1 (E.D. Tex. July 10, 2015); In the Matter of Orthofix International N.V., Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21c of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, Administrative Proceeding File No. 3-17800, Release No. 79828, https://www.sec.gov/litigation/admin/2017/34-79828.pdf; Press Release, SEC, Medical Device Company Charged with Accounting Failures and FCPA Violations (Jan. 18, 2017), available at https://www.sec.gov/news/press-release/2017-18.

[6] Extended Deferred Prosecution Agreement (Sept. 23, 2016), available at https://www.justice.gov/criminal-fraud/file/971416/download.

[7] Letter Regarding Extension of Deferred Prosecution Agreement (March 3, 2022), available at https://www.justice.gov/criminal-fraud/file/1518836/download.

[8] Press Release, Dep't of Justice, Aibel Group Ltd. Pleads Guilty to Foreign Bribery and Agrees to Pay $4.2 Million in Criminal Fines (Nov. 21, 2008), available at https://www.justice.gov/archive/opa/pr/2008/November/08-crm-1041.html.

[9] Press Release, Dep't of Justice, Zimmer Biomet Holdings Inc. Agrees to Pay $17.4 Million to Resolve Foreign Corrupt Practices Act Charges (Jan. 12, 2017), available at https://www.justice.gov/opa/pr/zimmer-biomet-holdings-inc-agrees-pay-174-million-resolve-foreign-corrupt-practices-act.

[10] Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime (Oct. 28, 2021), available at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.