

[Blogs](#)

October 13, 2022

Key Compliance Takeaways from Oracle's \$23M FCPA Settlement with the SEC



On September 27, 2022, the United States Securities and Exchange Commission (SEC) [announced](#) a settlement with Oracle Corporation (Oracle) to resolve allegations that its subsidiaries in India, Turkey, and the United Arab Emirates violated the Foreign Corrupt Practices Act (FCPA) by creating off-the-books slush funds and using those slush funds to bribe foreign government officials.

Without admitting or denying the SEC's findings, Oracle agreed to cease and desist from violating the anti-bribery, books and records, and accounting provisions of the FCPA and to pay approximately \$8 million in disgorgement and a \$15 million penalty.

Notably for both attorneys and companies, the SEC's order provides insights into how to design an effective corporate compliance program to minimize legal risk, including FCPA risk.

The SEC's Findings

The SEC [found](#) that, from at least 2014 to 2019, Oracle's subsidiaries in India, Turkey, and the United Arab Emirates "used discount schemes and sham marketing reimbursement payments" to finance slush funds, which were held by Oracle's "channel partners" (i.e., distributors and resellers) in those markets. The subsidiaries transacted through these channel partners during the relevant period under Oracle's indirect sales model, by which channel partners sell Oracle products to end customers. According to the SEC, the subsidiaries and the complicit channel partners used the slush funds—which employees of the subsidiaries referred to as the "buffer," "moneybox," "pool," and "wallet"—to bribe government officials in return for business. Specifically, the SEC determined that, among other things, (i) employees of Oracle Turkey and Oracle UAE used slush funds to pay for travel for government officials, including to Oracle's annual technology conference in California; (ii) an Oracle Turkey employee directed cash bribes to government officials; (iii) an Oracle UAE employee paid approximately \$130,000 in bribes to the chief technology officer of a state-owned entity (SOE) in return for six contracts in 2018 and 2019; (iv) Oracle India employees funneled \$330,000 to an entity known for paying

government officials; and (v) an Oracle India employee maintained a spreadsheet indicating that \$67,000 was available to make payments to a government official.

As detailed in the SEC's cease-and-desist order, the subsidiaries were able to finance the slush funds primarily for three reasons. First, employees of the subsidiaries were able to obtain larger discounts than required for legitimate business reasons, at least in part because Oracle did not require documentary support for discount requests. For example, the SEC found that Oracle approved a 70% discount on software for an Indian SOE based solely on representations from an Oracle India employee that there was intense competition for the tender. The SOE's website, however, indicated that Oracle did not face any competition because the SOE had mandated the use of Oracle software for the project.

Second, the complicit channel partners did not fully pass through the discounts to the end customers and used the excess margin to capitalize the slush funds.

Third, Oracle allowed employees of the subsidiaries to approve individual payments of less than \$5,000 to channel partners for marketing activities without any corroborating documentation showing that the activities occurred. The SEC's order notes that an Oracle Turkey employee approved numerous payments—which were supposedly for channel partners' marketing activities and were individually under the \$5,000 limit—totaling over \$115,000 in 2018.

Key Takeaways from a Compliance Perspective

Based on the SEC's findings, companies should reevaluate the adequacy of their compliance programs. The SEC's order makes clear that it expects companies to implement controls regarding discounts, purchase orders, business gratuities, and partners. Such controls should include:

- requiring employees to provide both legitimate business reasons and supporting documentation for discount requests, at least in indirect transactions;
- verifying that discounts are fully passed through to end customers;
- prohibiting employees from making payments to vendors for services (e.g., marketing) absent documentation showing that the vendors performed the agreed-upon work;
- limiting business gratuities to third parties, particularly government officials;
- vetting and monitoring partners; and
- terminating partners involved in misconduct.

Lastly, the SEC's findings highlight that companies can more effectively conduct internal investigations by identifying any unusual terms related to the conduct at issue (e.g., buffer, moneybox, pool, and wallet) and reviewing documents from relevant custodians that include those terms.

Authors

Explore more in

[White Collar & Investigations](#)