BRACEWELL

INSIGHTS

VimpelCom's Global FCPA Settlement - A Multinational Resolution

February 26, 2016

The U.S. Department of Justice (DOJ), the U.S. Securities and Exchange Commission (SEC) and the Public Prosecution Service of the Netherlands (OM) announced a coordinated criminal and civil Foreign Corrupt Practices Act (FCPA) resolution with VimpelCom, a Dutch telecommunications company. In total, VimpelCom agreed to pay $795 million in fines and disgorgement stemming from a seven-year bribery scheme in Uzbekistan. The $397.5 million U.S. portion of the settlement amounts to the fifth largest FCPA settlement. The VimpelCom resolution is anticipated to be the first in a succession of actions against other telecom companies that have operated in Uzbekistan, including TeliaSonera and Mobile TeleSystems.

VimpelCom, the world's sixth-largest telecommunications company, has securities publicly traded in New York. In an effort to enter the Uzbekistan telecom market, in 2006, VimpelCom purchased an Uzbek telecom company, Unitel LLC (Unitel), along with Bakrie Uzbekistan Telecom LLC (Buztel), a smaller company partially owned by an unidentified Uzbek government official who is reported to be Gulnara Karimova, the daughter of Uzbekistan's president. Having already raised FCPA red flags with the Buztel acquisition, VimpelCom allegedly began, through Unitel's executives and employees, a multi-year scheme to bribe the highly influential foreign official through structured and concealed payments. By 2012, Unitel may have paid more than $114 million in bribes to obtain telecommunications business in Uzbekistan. The public settlement documents state that bribes were disguised as various payments to a shell company that was beneficially owned by the foreign official.

In corresponding criminal informations, both VimpelCom and Unitel were charged with conspiring to violate the FCPA's anti-bribery and internal controls provisions. DOJ also filed two civil complaints seeking an additional $850 million in forfeiture, which are amounts alleged to be the proceeds of illegal bribes paid to the Uzbek official. The SEC filed a civil complaint, charging VimpelCom with violating the FCPA's anti-bribery provisions, books and records provisions, and internal controls provisions. On February 18, the agencies announced that VimpelCom entered into a deferred prosecution agreement (DPA) with the DOJ and settled with the SEC. In a corresponding action, Unitel entered into a plea agreement and pleaded guilty before U.S. District Judge Edgardo Ramos (S.D.N.Y.). After various inter-agency credits, the combined total amount of U.S. and Dutch criminal and regulatory penalties paid by VimpelCom will be $795,326,398.40, making it one of the largest global foreign bribery resolutions in history.

According to the government, the result for VimpelCom could have been worse. Although VimpelCom did not self-report, the company substantially cooperated with the investigations and undertook significant efforts to provide evidence and employees for interviews. In outlining

its relevant considerations for VimpelCom's DPA, the DOJ stated that VimpelCom provided "all relevant facts known to the Company, including information about individuals involved in the FCPA misconduct." VimpelCom received "full cooperation and remediation credit" for providing evidence uncovered during a previously conducted internal investigation. The company benefited from its "prompt acknowledgement of wrongdoing" and subsequent extensive remediation, which included the termination of wrongdoer-officers and -employees.

As part of its DPA, VimpelCom will conduct an overhaul of its compliance program. The company substantially upgraded its anti-corruption compliance program; retained new leaders of its legal, compliance, and financial gatekeeper functions; and committed to enhancing its compliance program and internal controls. VimpelCom is also required to retain an independent compliance monitor for a term of three years.

VimpelCom's failure to self-report the wrongful conduct it uncovered in its internal investigation, however, rendered a significant blow. DOJ deemed the company ineligible for a significant financial discount or a non-criminal disposition.

What does this mean for the telecom industry?

It may be tempting in this case to write off the VimpelCom scandal as just one egregious outlier in an otherwise relatively benign compliance landscape. But there are some important lessons to be taken from this case.

One: Update and review compliance policies thoroughly and often, especially when entering a new geographical market. Compliance teams and executive management should become knowledgeable of the foreign country's local laws, potential local content requirements and local customs that could be illegal or invite scrutiny. Local compliance programs or compliance reviews should be tailored to the specific risks associated with the industry and the region.

Two: Encourage broad and integrated understanding and acceptance of compliance policies, with appropriate checks and balances. VimpelCom's board members, executives, and employees all identified serious concerns with the company's practices, yet the company's internal controls still failed because of the obstructionist activity of certain management members. Don't let this happen. Create and foster a culture of compliance at all levels and across multiple departments. Reach out to accounting and IT personnel, the employees who may be best suited to identify and report potential books and records violations. Institute mechanisms whereby red flags can be reported at any rung of the corporate ladder, and create policy backstops that will frustrate attempts to bypass compliance requirements.

Three: Properly resource compliance programs. This involves not just time, money and staff, but also corporate culture. If entering a new geographical market, institute an on-the-ground compliance team or easy local access to compliance located elsewhere. Foster an environment whereby the Board and executive management inform and enforce compliance policies. Develop training modules specific to a new geographical market and require employees in the region to satisfy required training on a regular basis.