Anti-Corruption Report
An Acuris company

anti-corruption.com

October 2, 2019

ENFORCEMENT ACTIONS

Juniper Networks Resolves SEC Charges for $11.7M After Allowing Subsidiary Misconduct to Continue for Years

By Lori Tripoli, *Anti-Corruption Report*

California-based Juniper Networks, a networking and cybersecurity solutions company, has settled charges brought by the SEC claiming that the company violated the FCPA's internal controls and recordkeeping provisions. The problems stemmed from misconduct at Chinese and Russian subsidiaries involving leisure trips for customers, including some government officials, funded by off-the-books accounts and sometimes masked with the use of falsified meeting agendas. The SEC, which criticized the company's remedial efforts in Russia as ineffective, issued a cease-and-desist order (Order) requiring Juniper Networks to stop violating the FCPA and to pay disgorgement, prejudgment interest and a civil penalty totaling about $11.7 million.

"The Juniper Networks enforcement action is a reminder that third-party business partners and discounts are like the 'death and taxes' of the FCPA," observed Michelle Shapiro, a partner at Arent Fox. No matter how large, sophisticated and successful a company may be, "no one can totally avoid the inherent risks," she said. Companies need to recognize the risks and do all they can to mitigate them, Shapiro continued.

See our three-part series on managing subsidiary risks: "Setting Things Up for Success" (Mar. 29, 2017); "Culture and Communication" (Apr. 12, 2017); and "Internal Controls" (Apr. 26, 2017).

Troubles With Channel Partners in Russia and China

Failure to Shut Down Discounts

Salespeople in Juniper Networks' Russian subsidiary, JNN Development Corp. (JNN), secretly arranged with third-party channel partners to increase discounts on sales made through those channel partners but did not pass on the discounts to customers, the Order alleges. Instead, JNN employees and the channel partners used this off-the-books money to fund travel and marketing expenses to pay for leisure trips for customers, including some who happened to be government officials. Leisure trips to what the SEC called "international tourist destinations" such as Italy and Portugal ensued. Although JNN employees hoped to increase business as a result of this travel, the trips themselves were to places "where there were no Juniper facilities, industry specific

conferences, or other legitimate business justifications," the SEC wrote in its Order.

Although Juniper Networks learned about the off-book accounts and their uses in 2009, the inappropriate practices continued for another four years even though they were prohibited under company policies. "This case shows the important role senior management plays with respect to anti-corruption compliance," said Michael Casey, a partner at Kirkland & Ellis. Juniper Networks' "senior management failed to shut down improper conduct in a timely manner," he continued. "Indeed, the company's Russian subsidiary continued to use off-book accounts for several years after senior management first became aware of that practice," Casey noted.

Excessive Entertainment and Falsified Agendas

In about the same time span, from 2009 through 2013, salespeople at Juniper Networks' Chinese subsidiaries also paid for travel and entertainment of customers, including foreign officials, that the SEC deemed "excessive and inconsistent with Juniper policy." In addition, subsidiary marketing employees "falsified trip and meeting agendas for customer events that understated the true amount of entertainment involved on the trips," the SEC alleged.

Circumventing Policy

Juniper China's marketing staff also violated Juniper's policy requiring prior approval by Juniper's legal department of these events. "In violation of Juniper's policies and undermining its internal accounting controls over travel and entertainment, the Juniper Legal Department staff responsible for reviewing third-party hospitality within the Asia-Pacific region regularly approved events that had already been conducted despite the requirement that such events receive prior review and approval," according to the Order.

High-Risk Industry

Juniper's business activities carry a significant amount of risk, heightened by where the company operates. "Technology companies may be more susceptible to corruption along the lines of what transpired at Juniper Networks because of their expansion in developing markets, where corruption and bribery are often seen as the cost of doing business," said Megan Cunniff Church, a partner at MoloLamken. Employees' "ability to discount software and intellectual property to further [the company's] growth also make the hidden discounts and off-book accounts used for bribes or other improper incentives more of a possibility," she suggested.

No Anti-Bribery Charges

It is "noteworthy that despite the number of years Juniper Networks violated the internal accounting controls and recordkeeping provisions of the FCPA, there are no allegations that Juniper Networks violated the anti-bribery provisions of the FCPA," Church said.

"The underlying problem of having allowed excessive travel expenditures for end-customer representatives in Juniper might not have warranted, by itself, enforcement action let alone an almost $12-million settlement," noted Bruce Searby, a partner at Searby. "But clearly the use of a slush fund mechanism to circumvent anti-bribery policy and then Juniper's failure to adequately remedy the problem once it became known is what drove this case," he continued.

See also "EY's Rick Sibery Outlines a Seven-Step Process for Monitoring Third Parties" (Oct. 26, 2017).

An $11.7-Million Deal Following Cooperation and Remediation

Ultimately, Juniper Networks agreed to pay $4 million in disgorgement, a little over $1.2 million in prejudgment interest and a civil penalty of $6.5 million all without admitting or denying the SEC's findings. The SEC mentioned Juniper Networks' disclosure of facts developed during an internal investigation after the company learned of the SEC's own investigation. Juniper Networks also voluntarily produced and translated documents.

In a prospectus filed with the SEC, Juniper Networks noted that its "Audit Committee, with the assistance of independent advisors, conducted a thorough internal review of possible violations of the FCPA, and the Company made improvements in its internal controls and carried out a number of disciplinary actions."

Specifically, Juniper Networks revised compliance policies and realigned its compliance function into an integrated unit reporting to a chief compliance officer, a new position, the SEC order noted. In addition, Juniper Networks implemented a mandatory escalation policy to ensure its board of directors is informed about serious matters. The company also created an independent and expert investigations function and instituted mandatory due diligence and prior approval processes by its compliance department for channel partners and other vendors. Pre-approval of nonstandard discounts and of third-party gifts, travel and entertainment expenses, channel marketing expenses and certain operating expenses in high-risk markets is required. Juniper Networks also conducted additional anti-corruption training for employees and improved its processes for conducting internal investigations, the SEC reported.

The regulated community might take note of the remedial activities the SEC enumerated in the Order. The SEC's order "describes Juniper's remedial actions, like creating 'an independent and expert investigations function,' in more detail than is typical in SEC cease-and-desist orders," observed Coates Lear, a partner at Squire Patton Boggs who previously worked in the SEC's Division of Enforcement. "That suggests that the Commission approves of those actions and wants other companies to take note of them," Lear said.

One notable omission from the laundry list of remedial actions taken by Juniper Networks concerns its third parties' own compliance programs. "One thing that is not mentioned is a requirement that channel partners implement, monitor and enforce their own effective compliance programs to prevent the violation of applicable laws, regulations and industry codes," Shapiro said. "That requirement can and should be built into third-party contracts, but that should not be the end of the story," she continued.

Given that compliance "is a constant struggle for even the biggest and best-intentioned companies," helping to ensure that channel partners "have the training and resources necessary to fulfill their compliance obligations, and monitoring their compliance through mechanisms like annual certifications and periodic audits, is important," Shapiro said.

See also "Recent DOJ Alum Sandra Moser Discusses Maximizing Cooperation Credit" (Feb. 20, 2019).

An Unchastened SEC?

The SEC's effort against Juniper Networks is, in the minds of some, emblematic of its attitude toward enforcement. "The Juniper Networks enforcement action showcases the SEC's aggressive approach to alleged violations of the FCPA's accounting provisions," said Jane Shvets, a partner at Debevoise.

"We continue to see the ascendancy of the SEC in FCPA enforcement actions," observed William Steinman, a senior partner at Steinman & Rodgers. "The FCPA's accounting provisions are powerful enforcement tools, and unlike the anti-bribery provisions, they are subject to a strict liability standard," he noted. In other words, the SEC "does not have to show that a company or its personnel intended to maintain lax internal controls or make inaccurate entries in the company's books and records," Steinman said. FCPA accounting provisions cases "are relatively easy cases to prove, and the SEC has embraced this," he continued.

Even high profile FCPA actions like Walmart did not implicate the anti-bribery provisions of the statute.

See our three-part series on Walmart's settlement with the DOJ and SEC: "Walmart Finally Settles for $282M and a Monitor" (Jul. 10, 2019); "Analyzing Walmart's Unique Monitorship and Its Compliance Failures and Fixes" (Jul. 24, 2019); and "Lessons in Self-Reporting and Cooperation" (Aug. 7, 2019).

Reality Check for an Industry That Likes to Move Fast and Break Things

"The tech industry moves quickly, competition is often fierce and the drive for market share is intense," Steinman observed. Indeed, tech-giant Facebook's original motto was "move fast and break things." However, "the rules are still the rules, and the enforcement agencies have shown that they understand the industry and the particular corruption risks it faces," he said.

It is unclear whether Juniper Networks willfully ignored the goings-on in China and Russia. "A root cause of Juniper Networks' problems may have been apathy to compliance enforcement in the face of profitability," Church said. "As long as the company was meeting its sales numbers in China and Russia, no one looked too closely at how they were meeting those numbers," she explained.

"It is also possible that the company rationalized the off-book accounts, travel practices and discounts as the necessary costs of doing business in developing markets," Church noted. "The reward of the new business justified the risk of potentially getting caught by government regulators," Church said.

See "Channeling the Channel-Partner Risk: Addressing Anti-Corruption Risk with Channel Partners in the Technology Sector" (Jun. 21, 2017).

Recurrent Themes for Many Industries

"This is a resolution to pay attention to for all companies that operate in challenging jurisdictions, and Russia and China in particular," Shvets said, noting that the fact pattern described in the Order "is far from unique in these jurisdictions and likely not limited to a particular industry."

The challenges that Juniper Networks faced are those that many organizations encounter. "Technology companies are not uniquely susceptible to violating the FCPA," Casey said. "All companies risk violating anti-corruption laws that have operations, sales or counterparties in high-risk jurisdictions, utilize third parties to act on their behalf, and interact with foreign government officials," Casey continued.

Further, Juniper Networks' problems stemmed from distributors, an area of continuing interest to the SEC. "Starting in 2018, the SEC began to apply heightened scrutiny on how companies engage distributors and monitor their activities," Steinman said. "Among other things, the SEC has started to question how companies set distributor discounts and what distributors do with them," he noted. In the Juniper Networks matter, the SEC "faulted the company for approving increased discounts on a case-by-case basis but failing to confirm that all of the increase was passed along to end-user customers," Steinman observed. "The SEC has raised this issue in several other enforcement actions over the last 12 to 18 months, and companies should take note."

See "How the SEC May Circumvent the Five-Year Statute of Limitations on Disgorgement Under *Kokesh v. SEC*" (Aug. 16, 2017).

Legal Department Sign-Off

Juniper Networks' experience may also serve as a wake-up call of sorts for in-house counsel. According to the Order, Juniper's legal department, going against corporate travel policies, approved numerous trips without sufficient review and after the events had taken place.

"Juniper Networks' primary vulnerabilities were its lax oversight of business practices and accounts in Russia and China and an ill-equipped legal department that was tasked with compliance and procurement-approval functions," Church said. "Despite the company's knowledge of violations of its own policies, it allowed the off-book accounts and discounts to continue," she noted. "While there were efforts to deceive the legal department with falsified trip and meeting agendas, the legal department should have caught and ended the improper practices by, at a minimum, enforcing the company's policies."

Keeping Travel and Entertainment in Check

That said, providing travel and lodging to foreign officials is a standard business practice. Indeed, the FCPA specifically addresses "the provision of reasonable and bona fide hospitality," Steinman noted. "Officials often want to travel for training, factory acceptance tests, milestone reviews or just to kick the proverbial tires," he said. "The key is to develop appropriate controls over the practice and ensure that they are effective," Steinman continued.

Even as companies legitimately offer travel and hospitality to customers, "there is an inherent risk of so-called 'mission creep,'" Steinman said. "Business folks want to ensure that their customers are happy. They want their customers to like them. There's nothing wrong with that," he explained.

An effort to please customers can, however, get out of hand. "It often comes with the desire to push for business class instead of coach travel" or "a luxury hotel with a spa instead of a traditional business hotel" or "a stopover someplace fun" or "a lavish dinner at a hot restaurant," Steinman said. "What starts as a normal business trip can soon morph into something over the top, and that is when problems arise," he cautioned.

Audits of travel requests might have helped Juniper Networks; not only do they help identify instances of noncompliance, they also have a deterrent effect, Steinman said.

Pre-trip approval is also vital. "When companies seek to provide travel, lodging and other forms of hospitality to foreign government officials, their legal and compliance departments should carefully scrutinize the proposed plans to ensure that they are for a legitimate business purpose and the expenses are reasonable," Casey suggested. "If legal or compliance personnel authorize out-of-scope activities, they should ensure the requisite internal approvals have been secured and contemporaneously memorialize their decision and the underlying rationale in writing," he said.

If employees furnish travel, lodging or hospitality to foreign officials without prior approval, this should be treated as a compliance infraction," Steinman said. "The employees in question should be disciplined," he continued.

At the same time, lawyers are particularly likely to be aware that exceptions to strict compliance with any given policy may sometimes be warranted. "Generally, try to build into a compliance approval process at least a touch of flexibility to account for the fact that unforeseen circumstances are a fact of life," Shapiro suggested. For example, rather than requiring advance legal department approval of all trips, she might recommend including a safety valve, such as a provision that allows "in unique situations where pre-approval is impractical or impossible" for an event to be reported to the general counsel's office or compliance department within 48 hours. While such an exception may not have applied in situations like that experienced by Juniper Networks, Shapiro acknowledged, such safety-valve language in a policy would at least supply "some wiggle room to argue that 'after-the-fact travel approvals' do not necessarily give rise to a books-and-records violation," she noted.

See "The Right Role for Legal in Compliance" (Oct. 8, 2014).

The Need for Well-Crafted and Enforced Policies

The SEC's mention of legal department laxity "highlights the importance of enforcing written policies and procedures," Lear said. "Failing to do so will always draw the government's attention," he explained.

To that end, "one important step that companies can take to protect themselves is to look closely at their policies and make sure that those policies are clear and practically workable given the realities of the business," suggested Shvets. "The Juniper resolution

(as well as other recent ones) shows that the SEC will not hesitate to use a company's own policies against it when they are not followed," she said. "That means that companies should routinely train and monitor employees in legal and compliance functions," Shvets said.

Ultimately, a regulated community needs to avoid a compliance program that is merely on paper. "To the extent certain procedures are not practically workable for valid reasons, it is better to adjust the policies (provided they remain robust and designed to prevent and detect misconduct) than to allow them to be ignored," Shvets said.

See "Six Steps for Converting a 'Paper' FCPA Compliance Program Into a Pervasive Culture of Anti-Bribery Compliance (Part One of Two)" (Feb. 20, 2013); Part Two (Mar. 6, 2013).