Statement

Statement in the Matter of David Hansen

Commissioner Hester M. Peirce

April 12, 2022

Exchange Act Rule 21F-17(a), adopted in 2011 as part of the whistleblower program mandated by the Dodd-Frank Act, prohibits taking "any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications." The Commission's Order concludes that David Hansen, a co-founder of NS8, Inc. who held various positions in the company, including Chief Information Officer, violated Rule 21F-17(a). The alleged violation related to Mr. Hansen's response to concerns raised with him by an NS8 Employee that the company was overstating the number of paying customers. The Order does not explain what, precisely, Mr. Hansen did to hinder or obstruct[1] direct communication between the NS8 Employee and the Commission. Accordingly, I dissent from instituting the action and accepting the settlement.

The Order states that the NS8 Employee was concerned that "NS8 was overstating its number of paying customers, including that the customer data . . . used to formulate external communications—including to potential and existing investors—was false." After submitting a tip to the Commission, the NS8 Employee raised these concerns with Mr. Hansen and told Mr. Hansen "that unless NS8 addressed this inflated customer data, he would reveal his allegations to NS8's customers, investors, and any other interested parties." Mr. Hansen, who "understood that the . . . concerns involved a possible securities law violation," suggested to the NS8 employee that he raise his concerns to his supervisor or to NS8's CEO, and the employee conveyed his concerns to his supervisor later that same day. The supervisor then called Mr. Hansen, who then called NS8's CEO.

The Order has several sentences describing interactions between Mr. Hansen and the CEO and their subsequent actions, but the salient facts, as I see them,[2] are:

- The "CEO told Respondent that he [the CEO] removed NS8 Employee's administrator privileges to one system but kept read-only access 'so it looks like an error.'"
- Mr. Hansen told the CEO that the NS8 Employee's company-issued computer had a tool that permitted remote access, and that Mr. Hansen could "'watch what [the NS8 Employee] is doing [on his company-issued computer] if we care.'"[3]
- Mr. Hansen "used NS8's administrative account to access the NS8 Employee's company computer" and "then left the NS8 Employee's computer and password in the CEO's office."
- The CEO fired the NS8 Employee later in the week.

Although the Order states that "both took steps to remove the NS8 Employee's access to NS8's IT systems," the above list includes only two concrete actions by Mr. Hansen: (1) accessing the NS8 Employee's computer and (2) leaving the computer and password in the CEO's office. How did Hansen's actions as set forth in the Order remove

the NS8 Employee's access to the IT systems, let alone stand in the way of the NS8 Employee's direct communication with the Commission? In my view, they quite plainly did not.

At most, these actions affected the content of what the NS8 Employee could communicate, not whether he could communicate. Rule 21F-17(a) ensures the whistleblower's entitlement to speak directly to the Commission, and NS8 did not prevent the NS8 Employee from doing so. Actions that limit access to company data do not necessarily limit access to the Commission. Mr. Hansen's actions, as reported in the Order, did not hinder the NS8 Employee's communications with the Commission regarding his already-submitted tip.[4] Furthermore, the Order does not state that Mr. Hansen knew about the tip. If there were evidence that he knew of the tip, then his actions may have implicated Rule 21F-17(a) or the anti-retaliation rules.

A broad interpretation of Rule 21F-17(a) could prohibit companies from limiting employees' access to data. Limiting access to sensitive data is a common element in cybersecurity programs.[5] A plausible inference, based on the facts recited in the Order, is that Mr. Hansen was concerned about the NS8 Employee's threat to disclose confidential company data "to NS8's customers, investors, and any other interested parties." Rule 21F-17(a) by its plain terms applies only to communications with the Commission. We should not read it in a manner that complicates a company's ability to act to protect its data in the face of sweeping disclosure threats, even well-intentioned ones by concerned employees. Companies hold troves of data about their customers, assets, and business practices. They and their customers have a keen interest in protecting those data. We should not engage in an undisciplined interpretation and application of Rule 21F-17(a) that adds unnecessary legal risk to that burden.

I respectfully dissent.

---

[1] Impede means "to retard in progress or action by putting obstacles in the way; to obstruct; to hinder; to stand in the way of." Oxford English Dictionary (1971).

[2] The Order also states that the NS8 Employee used a password management system installed on his NS8-issued computer to save passwords both "to various NS8-related applications" and to "his personal email and other applications." Additionally, the Order states that the saved passwords were used to access his personal accounts "on his NS8-issued laptop" the same day Mr. Hansen left the computer in the CEO's office. Because the Order does not identify who accessed what personal accounts, the relevance of these facts is not clear.

[3] The Order does not state that Mr. Hansen (or anyone else) in fact watched.

[4] The Order states that it was the CEO who limited the NS8 Employee's "privileges to one system" to "read-only access" and later fired the NS8 Employee, and does not state that Mr. Hansen had any role in either action.

[5] *See, e.g.*, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Rel. No. 34-94197, https://www.sec.gov/rules/proposed/2022/33-11028.pdf (proposing rule § 275.206(4)-9(a)(2)(4) to require as "an element of an adviser's or fund's reasonably designed policies and procedures . . . [r]estricting access to specific adviser or fund information systems or components thereof and adviser or fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or fund").