Use of Third-Party Email Accounts by Outside Directors or Others Could Waive Privilege

February 2, 2021 Matthew Fry, Jennifer Wisinski

PRACTICES Litigation, Corporate, Capital Markets and Securities, Securities and Shareholder Litigation, Private Equity

Outside directors, private equity managers, and others often use third-party email accounts to conduct business for the companies they oversee and manage. For example, an outside director of Company X may also serve as an executive officer of Company Y. An issue could potentially arise if the outside director sends or receives email communications relating to Company X via an email account set up by Company Y. A recent decision from the Delaware Chancery Court indicated that the use of third-party email accounts could result in a waiver of privilege over communications with company counsel in certain circumstances if the third-party's internal policies reserved the right to monitor emails transmitted through the accounts. This decision could have significant implications for those that use email accounts from third-party companies (including affiliates) to carry out their roles and responsibilities.

Background and Analysis

In re WeWork Litigation[1] involved litigation between SoftBank, WeWork, and WeWork minority shareholders. SoftBank maintained a significant ownership stake in WeWork and entered into a share purchase transaction by which it would acquire additional WeWork stock. The deal fell through, and WeWork and minority shareholders alleged SoftBank breached the master transaction agreement.

In addition to owning a substantial stake in WeWork, SoftBank owned approximately 84% of Sprint. SoftBank's COO served as chairman for both Sprint and WeWork, and Sprint's CEO assisted SoftBank's COO on matters related to WeWork. In discovery, WeWork sought certain documents and emails involving SoftBank's inhouse and outside counsel that were sent to or from the Sprint email accounts for SoftBank's COO and Sprint's CEO. The documents and emails related solely to SoftBank business and did not concern Sprint. SoftBank originally withheld these documents on attorney-client privilege grounds.

The Delaware Chancery Court held privilege over the emails was waived under the specific circumstances of the case, in large part due to use of the Sprint email accounts. Sprint's Code of Conduct stated "[e]mployees should have no expectation of privacy in information they send, receive, access or store on any of Sprint's computer systems or networks" and "Sprint reserves the right to review workplace communications (including but not limited to Internet activity, email, instant messages, social media or other electronic messages, computer storage and voicemail) . . . at any time." The court also noted that it could be inferred Softbank's COO and Sprint's CEO were aware of this policy when they sent and received the emails at issue. Applying a four-factor test borrowed from the employment law context to the unique facts of the case, the court held SoftBank's COO and Sprint's CEO "could not have had a reasonable expectation of privacy when they used their Sprint email accounts to share [SoftBank] information, the subject matter of which concerned WeWork and had nothing to do with Sprint." Finding there could be no reasonable expectation of

privacy, the court held that SoftBank's COO and Sprint's COO "failed to ensure the confidentiality of [SoftBank's] privileged information" and thus waived privilege over the documents at issue.

Implications and Steps to Protect Privilege

The use of third-party email accounts by outside directors (and others with dual roles) to conduct company business is common and widespread, and so are corporate policies to monitor emails transmitted through those accounts. After the *WeWork* case, this practice can put privilege protections over sensitive board documents, communications, and information in jeopardy in certain situations. Here are possible steps companies can take to strengthen privilege protections and avoid the risk of waiver:

- Review whether outside directors or others within the company currently use email accounts supplied by third-parties that reserve a right to review and monitor those accounts.
- Implement a policy that outside directors and others use only company email accounts for company business.
- Implement a policy that outside directors and others not use another company's email account for company business.
- If not using company email accounts, instruct outside directors to use personal webmail accounts and/or to encrypt their communications.
- Make use of secure data portals through which outside directors send and receive sensitive company documents and information.
- Secure agreements with the third-parties supplying the email accounts that exempt the outside directors' and others' email accounts from monitoring policies or otherwise limit the rights of the third-parties to review and monitor the outside directors' and others' accounts.

Some of these steps may be more practical than others depending on each situation.

Courts in other jurisdictions (or even other courts in Delaware) and in other situations may reach an outcome different than the *WeWork* decision. And many times, there will be several arguments a proponent of privilege could make to ward off assertions of waiver, even with a similar set of facts. For instance, the court specifically noted communications shared between a parent corporation and its wholly-owned subsidiary would involve a different set of facts not at issue in the case. The court also pointed out specific problems with certain agreements between SoftBank and Sprint that supported the ruling. Nevertheless, corporate legal departments and private equity principals should take note of the *WeWork* case and be proactive in mitigating the risk of waiver.

---

[1] 2020 WL 7624636, at *2 (Del. Ch. Dec. 22, 2020).