New SEC Guidance on Safeguards to Protect Information Delivered to Holders of Securities Issued under Compensation Plans

On Nov. 6, 2017, the Securities and Exchange Commission (the "SEC") provided guidance on the use of safeguards to protect financial statements and other sensitive information delivered to holders of securities issued under written compensatory benefit plans under Securities Act Rule 701(e). The new guidance provides insight into permissible safeguards to protect information delivered both electronically and physically.

Rule 701 Summary

Rule 701 exempts from the Securities Act's registration requirement private company securities issued under written compensatory benefit plans to employees, consultants, advisors and others, such as options and restricted stock. The exemption is particularly helpful where a company desires to grant compensatory equity awards to recipients who are not accredited investors. Under Rule 701, the amount of securities a company may sell during any consecutive 12-month period is limited to the greater of (i) $1 million, (ii) 15 percent of its total assets, or (iii) 15 percent of the outstanding amount of the class of securities offered and sold in reliance on Rule 701.

Under Rule 701(e), a company must deliver to investors a copy of the compensatory benefit plan under which the securities are issued. If over $5 million is issued during any consecutive 12-month period, a company also must deliver additional information, including financial statements, before the date of sale.[1] A company may elect to deliver this information electronically or in physical form.

New Guidance

The SEC's new guidance in Securities Act Rules Compliance and Disclosure Interpretation 271.25 (available **here**) authorizes the use of "standard electronic safeguards, such as user-specific login requirements and related measures" when electronically delivering Rule 701(e) information. However, "[t]he use of a particular electronic disclosure medium either alone or in combination with other safeguards should not be so burdensome that intended recipients cannot effectively access the required disclosures." The new guidance exemplifies that, if a company elects to use a dedicated physical disclosure room to house the medium used to convey the information required to be disclosed, such room would need to be accessible during ordinary business hours upon reasonable notice. Further, "[o]nce access to the required information has been granted ... the medium used to communicate the required disclosure should provide the opportunity to retain the information or have ongoing access substantially equivalent to personal retention."

Practical Implications

Private companies have a legitimate interest in protecting their financial statements and other information delivered under Rule 701(e) from becoming publicly available as a result of unauthorized access from the outside as well as "leaks" from the inside. The safeguards employed should protect information available both in electronic and physical forms. The SEC's new guidance appears to stand for the proposition that, regardless of whether the Rule 701(e) information is in electronic or physical form, a company may employ safeguards to protect Rule 701(e) information so long as the safeguards are not effectively preventing access to the information. As a result, a company would have to evaluate the facts and circumstance in determining whether a particular safeguard results in adequate access and disclosure.

Some considerations in that respect include:

- A company should require recipients of Rule 701 securities to enter into confidentiality agreements as a condition to receipt of the securities.
- A company should consider restricting access to Rule 701(e) information, such as imposing password protection of electronic information and using designated and monitored media rooms for physical information. However, the use of a centrally located media room alone may be unreasonable if not all potential recipients work in the same building.
- A company should consider restricting recipients' ability to disseminate the information by preventing copying. However, the permitted degree of restriction is uncertain since the SEC's guidance expressly notes that the medium used must provide an opportunity to retain the information or have ongoing access substantially equivalent to personal retention.

With the increased risks associated with data breaches and the SEC's focus on cybersecurity risks, companies should consider potential safeguards and the SEC's new guidance in the context of its overall cybersecurity strategy, ensuring that they have implemented a legally compliant privacy and cybersecurity program, which takes into account not only SEC guidance, but also applicable federal, state, international and industry requirements and best practices. Experienced outside counsel can assist companies in developing and implementing this framework and can also help companies prepare for and respond to regulatory investigations, civil litigation and/or criminal litigation. In today's threat environment, the question is not "if" a breach will occur, but "when." Are you prepared?

If you have questions about the SEC's new guidance, please contact a member of Brownstein's **Securities**, **Cybersecurity** or **Employee Benefits** practice groups.

Rikard D. Lundberg
Shareholder
rlundberg@bhfs.com
303.223.1232

Nancy A. Strelau
Shareholder
nstrelau@bhfs.com
303.223.1151

Tracy L. Lechner
Shareholder
tlechner@bhfs.com
303.223.1274

Trayton D. Oakes
Associate
toakes@bhfs.com
303.223.1295

[1]It is likely that the $5 million will be increased to $10 million in the foreseeable future.