



Court Refuses to Compel Employees to Disclose Passcodes for Employer-Issued Smartphones

Insights

9.25.15

Just this week, in *Securities and Exchange Commission v. Huang*, No. 15-269 (E.D. Pa. September 23, 2015), the United States District Court for the Eastern District of Pennsylvania denied the Securities and Exchange Commission's request that the Court order two former credit-card issuer bank ("Bank") employees accused of insider trading to disclose the secret personal passcodes for smartphones owned by their former employer.

The SEC's Motion to Compel Production of the Passcodes

The SEC, believing the smartphones contained documents belonging to the Bank, issued a discovery request to the Defendants asking them to disclose the passwords for their Bank-owned smartphones. The Defendants refused, invoking their Fifth Amendment protections. The SEC filed a motion to compel production of the passcodes, arguing that as former employees, the Defendants were merely corporate custodians in charge of corporate records, and therefore could not assert a Fifth Amendment privilege in refusing to disclose the codes. The Defendants disagreed, arguing that they were not corporate custodians and that providing the passcodes would be "testimonial" in nature, permitting them to assert Fifth Amendment protections against such disclosure.

The Court's Ruling

The Court agreed with the Defendants, finding that since the SEC was seeking Defendants' personal thought processes, rather than business records, the Defendants could properly invoke their Fifth Amendment protections. In the course of reaching its decision, the Court noted that the SEC had submitted no evidence that the smartphones actually contained Bank-owned documents. The Court also observed that the Bank did not assign passcodes to its employees for use on Bank-issued smartphones, nor did it keep track of Defendants' passcodes. To the contrary, the Bank asked employees not to keep records of their passcodes for safety reasons.

Implications for Employers

The Court's comments regarding the Bank's failure to assign or keep records of employees' passcodes suggest that the decision may have had a different outcome if the Bank had maintained different policies regarding the passcodes. Although the nature of the Bank's instruction to employees not to keep records of their passcodes was not specified in the ruling, presumably, the Bank maintained this policy to further protect Bank data and ensure that the theft of a Bank-issued smartphone would be less likely to result in the loss of Bank information stored on the device. The Court's ruling suggests that in doing so, the Bank may have inadvertently waived its right to access

the data stored on its own smartphones. In light of the Court's ruling, employers may want to review corporate policies regarding the use and maintenance of passcodes for employer-issued devices, and also may want to consider whether to actively seek out and securely record those passcodes to facilitate access to information stored on the devices if necessary when company-issued devices are returned by employees.

Related People



Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
[Email](#)