Davis Polk

Securities Fraud Class Action Suits Following Cyber Breaches: The Trickle Before the Wave

December 21, 2017 | Client Update | 2-minute read

Large-scale data breaches can give rise to a host of legal problems for the breached entity, ranging from consumer class action litigation to congressional inquiries and state attorneys general investigations. Increasingly, issuers are also facing the specter of federal securities fraud litigation.

The existence of securities fraud litigation following a cyber breach is, to some extent, not surprising. Lawyer-driven securities litigation often follows stock price declines, even declines that are ostensibly unrelated to any prior public disclosure by an issuer. Until recently, significant declines in stock price following disclosures of cyber breaches were rare. But that is changing. The recent securities fraud class actions brought against Yahoo! and Equifax demonstrate this point; in both of those cases, significant stock price declines followed the disclosure of the breach. Similar cases can be expected whenever stock price declines follow cyber breach disclosures.

The claimed damages associated with a putative securities class action can be catastrophically large—driven by the size of the stock price decline and the volume of trading in an issuer's stock. The risks associated with such cases are therefore significant. But there are also a number of ways to successfully defend against them, both at the motion to dismiss phase—before issuers are exposed to the expense and distraction of discovery—and, if necessary, at later stages in the case.

Issuers should be thinking proactively about this risk. A company can strengthen its defense and help to protect itself against securities class action litigation by carefully attending to disclosure issues ***before*** any disclosure of a cyber breach and, indeed, before a breach ever happens. While companies will not be able to eliminate completely the risk of being subject to a securities fraud action related to cyber security, careful attention to these issues may reduce the risk, increase the possibility of early dismissal of such actions, and/or mitigate the potential scope of damages and costs associated with defending the litigation.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Michael S. Flynn
+1 212 450 4766
michael.flynn@davispolk.com

Joseph A. Hall
+1 212 450 4565
joseph.hall@davispolk.com

Edmund Polubinski
+1 212 450 4695
edmund.polubinski@davispolk.com

Neal Potischman
+1 650 752 2021
neal.potischman@davispolk.com

Brian S. Weinstein
+1 212 450 4972
brian.weinstein@davispolk.com

Related materials

2017-12-21_securities_fraud_class_action_suits_following_cyber_breaches_trickle_before_wave.pdf