Analysis

Facebook's $100M SEC Settlement May Complicate Libra Pitch

By Rachel Graf

Share us on: By Rachel Graf

Law360 (July 24, 2019, 8:39 PM EDT) -- The U.S. Securities and Exchange Commission's $100 million settlement Wednesday over Facebook's user data disclosures paved new ground for the securities regulator while amplifying concerns about the technology giant's privacy practices at a crucial time as it looks to launch a digital currency.

The SEC filed its complaint accusing Facebook Inc. of making misleading statements about research firm Cambridge Analytica's use of personal data just a week after lawmakers grilled the company about plans to develop a digital token, called Libra.

Consumer privacy is a central concern Facebook must address in the lead-up to Libra going live in the first half of 2020. The company has faced a flurry of lawsuits and congressional hearings delving into its various privacy lapses, including the Cambridge Analytica scandal. And a lawsuit over the scandal by one of the nation's top financial watchdogs will almost certainly exacerbate concerns about the planned currency, said Cornell Law professor Robert Hockett.

"It's not unusual, I don't think, for the Cambridge Analytica scandal itself to come into people's minds when they think about Libra," Hockett said. "And the SEC suit of course further underscores or puts a big neon light once again over that particular scandal."

Facebook's larger ambitions aside, the most recent lawsuit was squarely within the SEC's wheelhouse. The complaint alleged the company misrepresented to investors that the potential misuse of user data was hypothetical, even though the company knew a third-party developer had improperly sold the data of millions of users to political data firm Cambridge Analytica.

The SEC reached a similar deal over privacy disclosures with Altaba Inc. last year, resolving allegations that the Yahoo spin-out waited years to disclose that Russian hackers had stolen a massive amount of user data in 2014. But unlike Altaba, Facebook was never technically hacked. Instead, the SEC's complaint centered around disclosures about a third-party developer's improper transfer of user data.

"[The Facebook lawsuit] expands the notion of what could be a cyber-related issue," said Joseph Facciponti, a former federal prosecutor in Manhattan who now works at Murphy & McGonigle.

"It's not just a data breach or a cyber attack," he said. "The SEC also expects companies that are custodians of personal information to disclose issues related to customer privacy."

The settlements were reached at a time when the SEC has been sharpening its focus on cybersecurity. Shortly after Jay Clayton was sworn in as chairman in 2017, he established a new cyber unit and made cyber-related misconduct a priority.

To avoid any unwanted attention from the SEC, public companies should revisit the agency's 2018 guidance about how to disclose their cybersecurity risks, said Todd Cipperman, founding principal at the compliance firm Cipperman Compliance Services.

The guidance laid out factors and obligations issuers should consider when telling investors about material risks they face from hackers and cybercriminals and what an actual incident could mean for the company's health and ongoing operations. It also encouraged them to take certain specific steps, such as ensuring they have policies to prevent insider trading by executives and directors prior to a cyber incident becoming public.

Private companies should take notice as well, especially within the asset management industry where concerns about protecting customer information are especially common, Cipperman said.

"If you think the SEC doesn't care about this stuff, they just went after Facebook," Cipperman said. "So they certainly do."

The case is SEC v. Facebook Inc., case number 3:19-cv-04241, in the U.S. District Court for the Northern District of California.

--Additional reporting by Ed Beeson and Philip Rosenstein. Editing by Philip Shea and Michael Watanabe.

View comments

0 Comments