

DEPARTMENT OF FINANCIAL SERVICES CALLS FOR REGULATION OF SOCIAL MEDIA GIANTS AFTER TWITTER HACK INVESTIGATION

Report by Department Finds Twitter Lacked Adequate Cybersecurity Protections as Regulated Cryptocurrency Companies Acted Swiftly to Combat Impact of Hack

The New York State Department of Financial Services (DFS) today released a report on the [Department's investigation](#) into the July 15, 2020 hack into the Twitter accounts of cryptocurrency firms and well-known public figures, following [Governor Andrew M. Cuomo's](#) request to investigate the matter. Among DFS' findings: the global social media platform lacked adequate cybersecurity protections and, at the time of the attack, did not have a chief information security officer. The report recommends a new cybersecurity regulatory framework for giant social media companies.

“Social media platforms have quickly become the leading source of news and information, yet no regulator has adequate oversight of their cybersecurity. The fact that Twitter was vulnerable to an unsophisticated attack shows that self-regulation is not the answer,” said **Superintendent of Financial Services Linda A. Lacewell**. “As we approach an election in fewer than 30 days, we must commit to greater regulatory oversight of large social media companies. The integrity of our elections and markets depends on it. The swift and effective response of DFS-regulated cryptocurrency companies illustrates how effective regulation can foster innovation and growth, while also protecting consumers.”

In 2019, Twitter had more than 330 million average users per month. According to the [Pew Research Center](#), 71% of Americans on Twitter use the platform as a source for news, and 42% of Americans engage on Twitter to discuss politics. The Department is issuing this report to alert consumers and voters as they prepare to exercise their basic rights in American democracy, in one of the most consequential elections in generations.

The report focuses on the facts surrounding the Twitter hack, the reasons it occurred, and ways to prevent future incidents.

The Department found the following:

- The hackers accessed Twitter’s systems with a simple technique: by calling Twitter employees and claiming to be from Twitter’s IT department. After the hackers duped four employees into giving them their log-in credentials, they hijacked the Twitter accounts of politicians, celebrities, and entrepreneurs, including Barack Obama, Kim Kardashian West, Jeff Bezos, Elon Musk, and several cryptocurrency companies regulated by the Department – accounts with millions of followers.
- The hackers tweeted simple “double your bitcoin” messages, with a link to send payments in bitcoins. In the end, they stole over \$118,000 worth of bitcoins from consumers.
- The Department’s regulated cryptocurrency companies, Coinbase, Square, Gemini Trust Company, and Bitstamp responded quickly to block attempted transfers to the Bitcoin addresses the fraudsters used.
- Despite being a global social media platform boasting over 330 million average monthly users in 2019, Twitter lacked adequate cybersecurity protection. At the time of the attack, Twitter did not have a chief information security officer, adequate access controls and identity management, and adequate security monitoring – some of the core measures required by the Department’s first-in-the-nation cybersecurity regulation.

Considering social media’s increasingly critical role as a source of news and information, the ease of the Twitter hack shows Twitter’s vulnerability to an election-related hacking attempt. Twitter and other large social media companies have no dedicated federal or state regulator ensuring that their cybersecurity policies and programs adequately address the risks of their digital operating models. Instead, they are largely self-regulated and have no accountability for significant cybersecurity lapses as occurred in the Twitter hack.

The report recommends that the largest social media companies, whose platforms reach millions of people around the world, should be designated as systemically important institutions with prudent regulation to manage heightened cybersecurity risk.

The pace of innovation accelerates every day, and government must keep up to protect consumers and safeguard markets and institutions. The Department supports innovation balanced by regulation, as is the case with its licensed cryptocurrency companies.

These recommendations are critical to ensuring that the cybersecurity of global social media companies has oversight as they grow more systemically significant, and that they establish strong cybersecurity measures to secure their users' accounts, maintain consumer trust, and safeguard our business and political systems, including elections, from outside influences.

[A copy of the report can be found on the DFS website.](#)

###