October 15, 2020

New York DFS Calls for Regulation of Social Media Platforms

New York State Department of Financial Services Calls for Regulation of Social Media Platforms in Report on Investigation of Twitter Hack

SUMMARY

On October 14, 2020, the New York State Department of Financial Services (the "DFS") released a report regarding a July 2020 hack into the Twitter accounts of celebrities and cryptocurrency firms.[1] The report includes a proposal that calls for large social media companies to be designated as "systemically important," and to become subject to a dedicated, enhanced regulatory framework to manage cybersecurity risks. In the related release, New York's Superintendent of Financial Services Linda A. Lacewell notes: "As we approach an election in fewer than 30 days, we must commit to greater regulatory oversight of large social media companies."[2]

BACKGROUND

On July 15, 2020, a group of hackers took control of a number of Twitter accounts belonging to celebrities and cryptocurrency firms. The accounts were used to tweet a cryptocurrency scheme that resulted in the hackers stealing over $118,000 worth of Bitcoin. Shortly after the attack, Governor Andrew Cuomo instructed the DFS to investigate.[3] The DFS report includes details on how the hack was carried out, the timeline of the attack and the responses of DFS-regulated cryptocurrency firms. Importantly, the scope of the DFS report goes beyond a mere investigation into the facts of the Twitter attack and proposes a new regulatory framework for social media firms.

The broad proposal for expanded public oversight and regulation of cybersecurity practices at large social media firms is consistent with steps the DFS has taken in recent years to seek to establish itself as a regulatory leader in cybersecurity and cryptocurrency activities. Specifically, in 2015, the DFS issued

regulations that require all persons to obtain a "BitLicense" from the DFS prior to engaging in certain cryptocurrency activities involving New York State or its residents.[4] The BitLicense, among other requirements, imposes significant cybersecurity provisions on licensees. Further, in 2017, the DFS implemented a comprehensive cybersecurity regulation, which became effective on March 1, 2019 (the "Cyber Regulation") and applies to banks, insurance companies and other financial services companies regulated by the DFS.[5] In the report, the DFS states that the Cyber Regulation was the first of its kind and has served as a model for other regulators.

DISCUSSION

The DFS report calls for "a comprehensive cybersecurity regulation and an appropriate regulator for large social media companies." To support this proposal, the DFS notes that Twitter (Goliath) was "brought to its knees" by a "group of unsophisticated cyber crooks" (David). The DFS also notes the upcoming presidential election and the prevalence of social media as a news source as reasons why government action is needed now—noting that "[t]he integrity of our elections and markets depends on it." The DFS report provides the example of the role of DFS-regulated cryptocurrency firms in blocking thousands of transactions in the Twitter hack as evidence of the effectiveness of cybersecurity regulation. In the related press release, the DFS states its recommendations to establish a regulatory framework for giant social media companies are "critical" as the companies grow more systemically significant, and that the companies must establish strong cybersecurity measures "to secure their users' accounts, maintain consumer trust, and safeguard our business and political systems, including elections, from outside influences."

Proposal for Comprehensive Cyber Regulation. With respect to implementing a "comprehensive cybersecurity regulation," the report expresses the DFS' view that its Cyber Regulation has "established an effective regulatory approach and is a good model" for regulating social media companies. Among other things, the Cyber Regulation requires all DFS-regulated banks, insurance companies and other financial services institutions to have in place a robust cybersecurity program, including developing policies for data governance, access controls, system monitoring, third-party security, and incident response and recovery to notify the DFS of both successful and certain unsuccessful cybersecurity attacks; and to certify annually the institution's compliance with the Cyber Regulation.

Importantly, the report calls for regulation of social media companies to "go even further" than the Cyber Regulation, noting that the Cyber Regulation was "carefully designed to be flexible enough to apply to the thousands of companies regulated by the [DFS]." In contrast, the report states that regulation for social media firms "could be applied to a handful of large, complex, and technologically sophisticated corporations with a global footprint." As a result, the report calls for cybersecurity regulation for social media firms to be "both more detailed and require more security in high-risk areas" than the Cyber Regulation, including "enhanced regulation such as the provision of 'stress tests' to evaluate the social media companies'

susceptibility to key threats." Although the report does not include detailed information on the form of the proposed regulation, any such regulation would certainly impose numerous and burdensome requirements on social media companies.

Proposal for a New Oversight Council. With respect to an appropriate regulator, the report notes that, although social media companies are subject to generally applicable laws, including data privacy laws such as the California Consumer Privacy Act and the New York State SHIELD Act,[6] they are largely self regulated and currently do not have a dedicated regulator to address cybersecurity issues, and calls for that "regulatory vacuum [to] be filled." The report puts forward a proposed system by analogy to the oversight of systemically important financial institutions ("SIFIs"). Under that system, SIFIs are designated by the Financial Stability Oversight Council based on a number of factors and are subject to enhanced regulatory supervision. The DFS asserts that the risks posed by social media to "consumers, economy, and democracy are no less grave than the risks posed by large financial institutions," and that the "scale and reach of [social media] companies, combined with the ability of adversarial actors who can manipulate these systems, require a similarly bold and assertive regulatory approach." Accordingly, the report proposes the establishment of a new "Oversight Council" that would identify "systemically important social media companies" based on "the reach and impact of social media companies, as well as the society-wide consequences of a social media platform's misuse." Any social media company designated as "systemically important" would then be subject to enhanced regulation and the oversight of "an expert agency" that has "deep expertise in areas such as technology, cybersecurity, and disinformation."

The DFS does not directly propose that the DFS or any other specific agency should be the "expert regulator" under the proposed framework, but rather states only that the regulator "could be a completely new agency or could reside within an established agency or at an existing regulator." The DFS has, however, sought to establish itself as a leader in the areas of cryptocurrency and cybersecurity regulation and, as stated in the DFS report, believes that its regulations provide an appropriate model for the proposed social media regulations. The DFS' proposal would appear to require legislative action to establish the proposed oversight council and appropriate regulator, and it remains to be seen whether the proposal will gain traction with either federal or state legislatures, and what role, if any, the DFS would have under the proposed regulatory framework. However, given the DFS' action to become a regulatory leader in the area and its past stance on the role of state regulators, it is reasonable to expect that the DFS will seek to have some role in any new regulatory regime.

* * *

[1] DFS, Twitter Investigation Report: Report on the Investigation of Twitter's July 15, 2020 Cybersecurity Incident and the Implications for Election Security (Oct. 14, 2020), *available at* https://www.dfs.ny.gov/Twitter_Report.

[2] DFS, Press Release, 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 (Oct. 14, 2020), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202010141.

[3] New York State Governor's Press Office, Governor Cuomo Directs State to Conduct Full Investigation of Twitter Hack (July 16, 2020), *available at* https://www.governor.ny.gov/news/governor-cuomo-directs-state-conduct-full-investigation-twitter-hack.

[4] N.Y. COMP. CODES R. & REGS. tit. 23, § 200.0, *et seq*.

[5] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.0, *et seq*. For additional details on the Cyber Regulation, see our Memorandum to Clients, dated January 3, 2017, *available at* https://www.sullcrom.com/dfs-issues-updated-proposed-cybersecurity-regulations.

[6] New York's SHIELD (or Stop Hacks and Improve Electronic Data Security) Act was enacted in 2019 and applies to all businesses that own or license computerized data that include private information of a New York resident. The SHIELD Act imposes enhanced data breach notification requirements and mandates "reasonable" cybersecurity safeguards, but does not specify controls or require a comprehensive cybersecurity program.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Thomas C. Baxter Jr.	+1-212-558-4324	baxtert@sullcrom.com
Whitney A. Chatterjee	+1-212-558-4883	chatterjeew@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Michael T. Escue	+1-212-558-3721	escuem@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Wendy M. Goldberg	+1-212-558-7915	goldbergw@sullcrom.com
Joseph A. Hearn	+1-212-558-4457	hearnj@sullcrom.com
Shari D. Leventhal	+1-212-558-4354	leventhals@sullcrom.com
Mark J. Menting	+1-212-558-4859	mentingm@sullcrom.com
Nadar A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Camille L. Orme	+1-212-558-3373	ormec@sullcrom.com
Stephen M. Salley	+1-212-558-4998	salleys@sullcrom.com
Richard A. Pollack	+1-212-558-3497	pollackr@sullcrom.com
Rebecca J. Simmons	+1-212-558-3175	simmonsr@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Donald J. Toumey	+1-212-558-4077	toumeyd@sullcrom.com
Marc Trevino	+1-212-558-4239	trevinom@sullcrom.com

Benjamin H. Weiner	+1-212-558-7861	weinerb@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
William F. Kroener III	+1-202-956-7095	kroenerw@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Kamil R. Shields	+1-202-956-7040	shieldsk@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Andrea R. Tokheim	+1-202-956-7015	tokheima@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
William F. Kroener III	+1-310-712-6696	kroenerw@sullcrom.com
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
London		
Richard A. Pollack	+44-20-7959-8404	pollackr@sullcrom.com
Evan S. Simpson	+44-20-7959-8426	simpsone@sullcrom.com
Palo Alto		
Nadar A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com
Tokyo		
Keiji Hatano	+81-3-3213-6171	hatanok@sullcrom.com