

COMMITTEE ON OVERSIGHT AND REFORM

SUBCOMMITTEES:

NATIONAL SECURITY, RANKING MEMBER

GOVERNMENT OPERATIONS

CIVIL RIGHTS AND CIVIL LIBERTIES

COMMITTEE ON NATURAL RESOURCES

SUBCOMMITTEES:

NATIONAL PARKS, FORESTS, AND PUBLIC LANDS

WATER, OCEANS, AND WILDLIFE

POLICY COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515-1010

JODY B. HICE

10TH DISTRICT, GEORGIA

HICE.HOUSE.GOV

409 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4101

100 COURT STREET
MONROE, GA 30655
(770) 207-1776
(770) 266-6751 FAX

3015 HERITAGE ROAD, SUITE 6
MILLEDGEVILLE, GA 31061
(478) 457-0007
(478) 451-2911 FAX

210 RAILROAD STREET, ROOM 2401
THOMSON, GA 30824
(706) 969-1461

July 20, 2020

Jack Dorsey
Chief Executive Officer
Twitter
355 Market Street, Suite 900
San Francisco, CA 94103

Dear Mr. Dorsey,

On July 15, 2020, as you are undoubtedly aware, Twitter suffered a significant and widespread security incident. The cyberattack affected a large number of accounts while several additional accounts, including those of former President Barack Obama, Democratic Presidential candidate Joe Biden, Elon Musk, Apple, and Uber, were used to post a cryptocurrency scam¹ that sent over \$115,000 in transactions to an anonymous Bitcoin wallet.² While investigations are ongoing, the Twitter Support account on your platform indicated that same day you believe the incident to be a “coordinated social engineering attack” perpetrated on Twitter employees who had access to critical internal controls and toolsets.³

We do not doubt that the security of your platform, its users, and that of your employees is of the utmost importance to you and we are sure you are taking the necessary steps to not only secure your systems but to set in place protocols which will deter such an incident from happening again in the future. However, as you know, the President of the United States, numerous agencies of the United States federal government, all branches of the United States Armed Services, all Members of the United States Senate, and the majority of Members of the United States House of Representatives have accounts on your platform to engage in communication with our Nation’s citizens and individual constituents. These accounts are used to present accurate and unfiltered information to the American people, and their security cannot be understated.

Additionally, we are further concerned with widespread media reports of screenshots featuring Twitter moderator tools.⁴ Twitter repeatedly deleted images of the leaked toolset posted

¹ Nick Statt, *Barack Obama, Joe Biden, Elon Musk, Apple, and others hacked in unprecedented Twitter attack*, THE VERGE (July 15, 2020), <https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised>.

² David Ingram & Kevin Collier, *Biden, Gates, Musk: Bitcoin scam breaches some of the world’s most prominent Twitter accounts*, NBC NEWS (July 16, 2020), <https://www.nbcnews.com/tech/security/suspected-bitcoin-scammers-take-over-twitter-acchttps://www.floridatoday.com/story/tech/science/space/2020/07/15/accounts-like-elon-musk-and-bill-gates-hacked-bitcoin-twitter-breach/5446449002/ounts-bill-gates-elon-n1233948>.

³ Twitter Support (@TwitterSupport), Twitter (July 15, 2020), <https://twitter.com/TwitterSupport/status/1283591844962750464>.

⁴ Joseph Cox, *Hackers Convinced Twitter Employee to help Them Hijack Accounts*, VICE NEWS: MOTHERBOARD (July 15, 2020), https://www.vice.com/en_us/article/jgxd3d/twitter-insider-access-panel-account-hacks-biden-uber-bezos.

to your platform and in some cases suspended accounts for posting the images due to a claim they violate the platform's rules.⁵ While I believe the perpetrators of this crime should be prosecuted to the fullest extent of the law for their wrongdoings, we are additionally disturbed by the revelation of buttons labeled "SEARCH BLACKLIST" and "TRENDS BLACKLIST" within the leaked images of the purported Twitter toolset.

On September 5, 2018, you testified at a hearing held by the House of Representatives Committee on Energy and Commerce that, "Twitter is used as a global town square, where people from around the world come together in an open and free exchange of ideas. We must be a trusted and healthy place that supports free and open discussion."⁶ You further stated, "[l]et me be clear about one important and foundational fact: Twitter does not use political ideology to make any decisions, whether related to ranking content on our service or how we enforce our rules."⁷ During this hearing, you repeatedly confronted concerns related to account shadow-bans and the manipulation or blacklisting/denylisting of trending topics by stating that Twitter's algorithms have no inherent political bias. However, while it may be true that Twitter's algorithms act neutrally, you failed to report to committee members whether manual tools exist that may be used by your employees to shadow-ban or manipulate accounts or trending topics.

As you yourself noted, the "town square" has moved online, and the free exchange of ideas is paramount to a diverse and thriving society of which those individuals may also place trust in your company for the protection of their personal information. To further understand the extent of the breach and the Twitter toolset, please provide written answers to the following questions:

- Did the breach occur due to a vulnerability in Twitter systems architecture or a social engineering scheme?
- How many accounts were compromised by the breach?
- What data, including personal records, were compromised?
- If official government accounts were compromised, what agencies or individuals were affected?
- What is the intent and use of the manual tools "SEARCH BLACKLIST" and "TRENDS BLACKLIST"?
- What other manual tools does Twitter employ beyond "SEARCH BLACKLIST" and "TRENDS BLACKLIST"?
- Have these manual tools ever been used to shadow-ban accounts or manipulate or de-list trending topics on your platform?


Should you have any questions, please contact my office at (202) 225-4101 or my Legislative Director, Nicholas Brown, at Nicholas.Brown@mail.house.gov. Thank you for your attention to this inquiry.

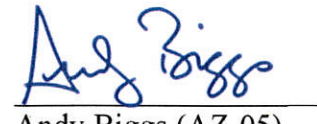
Sincerely,

⁵ *Id.*

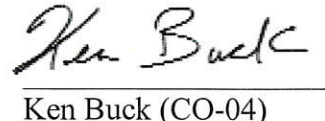
⁶ *Twitter Transparency and Accountability: Hearing Before H. Comm. on Energy & Commerce, 116th Cong.* (Statement of Jack Dorsey, Chief Exec. Officer, Twitter).


⁷ *Id.*



Jody Hice (GA-10)
Member of Congress

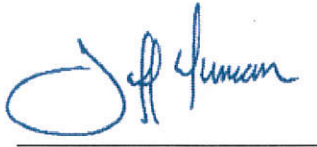

Andy Biggs (AZ-05)
Member of Congress



Dan Bishop (NC-09)
Member of Congress

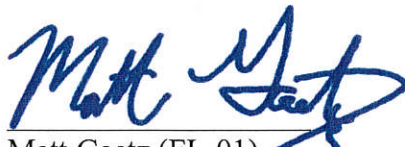

Ken Buck (CO-04)
Member of Congress

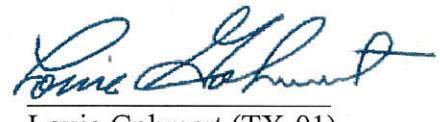

Ted Budd (NC-13)
Member of Congress



Michael Cloud (TX-27)
Member of Congress


Jeff Duncan (SC-03)
Member of Congress



Russ Fulcher (ID-01)
Member of Congress



Matt Gaetz (FL-01)
Member of Congress

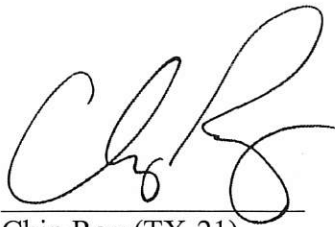

Louie Gohmert (TX-01)
Member of Congress


Paul A. Gosar, D.D.S.
Member of Congress


Debbie Lesko (AZ-08)
Member of Congress


Ralph Norman (SC-05)
Member of Congress



Scott Perry (PA-10)
Member of Congress



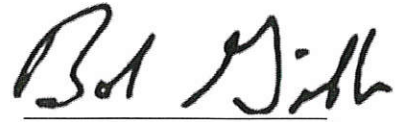
Chip Roy (TX-21)
Member of Congress



W. Gregory Steube (FL-17)
Member of Congress



Ron Wright (TX-06)
Member of Congress



Bob Gibbs (OH-07)
Member of Congress



Guy Reschenthaler (PA-14)
Member of Congress