March 16, 2023

The Honorable Lina M. Khan, Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
lkhan@ftc.gov

Dear Chair Khan,

On February 15, 2023, Twitter announced their planned update to the platform's two factor authentication (2FA) for users that are not subscribed to Twitter Blue.[1] Previously, any account that opted in to 2FA could use any of three options to secure their account: text messaging, authentication app, or security key. After March 20, 2023, users not paying the Twitter Blue subscription will not be able to use the text messaging option, and accounts that have not switched to a different method will have 2FA disabled. NHMC believes this decision is an unfair and deceptive act that essentially forces users to pay for security on the platform. This is yet another example of pay-to-play policies, like paywalls more generally, that create and exacerbate digital inequities and prevent historically and intentionally marginalized groups like Latinos from fully and safely utilizing the internet.[2] Twitter purports to be a platform that "give[s] everyone the power to create and share ideas and information instantly without barriers."[3] Yet, this latest decision is a barrier to create and share securely. NHMC urges the Federal Trade Commission (FTC) to take action on this most recent violation of the law by Twitter to hold the platform accountable for the security and fair treatment of its users.

According to the FTC, "unjustified consumer injury" alone can "warrant a finding of unfairness."[4] NHMC believes that the decision to put the most accessible form of 2FA behind a paywall will lead to unjustified consumer injury in the form of decreased security for accounts not subscribed to Twitter Blue. Unfortunately, the consumers most impacted by this new policy will be lower income users who are unable to pay for subscriptions. This includes many Latino

[1] Twitter Inc., *An update on Two-Factor Authentication Using SMS on Twitter*, (15 February 2023), https://blog.twitter.com/en_us/topics/product/2023/an-update-on-two-factor-authentication-using-sms-on-twitter ("Twitter Updated Policy").
[2] *Solutions on the Digital Divide: Moving Toward an Equitable Future* https://ctu.ieee.org/solutions-to-the-digital-divide-moving-toward-a-more-equitable-future/ (last visited Mar. 15, 2023) ("Solutions on the Digital Divide").
[3] *Twitter Investor Relations FAQ* https://investor.twitterinc.com/contact/faq/default.aspx#:~:text=back%20to%20top-,What%20is%20Twitter's%20mission%20statement%3F,a%20free%20and%20global%20conversation (last visited Mar. 15, 2023).
[4] Michael Pertschuk et al., *FTC Policy Statement on Unfairness*, para 8, (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.

communities and others who already face harmful content paywalls, and are now being dealt security paywalls.[5]

In their announcement of this policy decision, Twitter recommends that users continue to use 2FA by switching to the authentication app or security key methods.[6] However, users are highly incentivized to turn off 2FA altogether because the other methods require many more steps to activate than a simple text.[7] The authentication app method requires users to find, download, and sometimes pay for an app and then link it to Twitter by scanning a QR code. The security key option is even more cumbersome as it involves paying for a physical key to log into Twitter. For many users, it will be much easier to turn off 2FA, at least for a short period of time, or they will have it automatically turned off for them, thereby decreasing the total number of users protected by any form of 2FA.

The incentive to disable 2FA is increased by the fact that Twitter's messages informing users of this change seem to threaten users with loss of access to their accounts if they don't take action: "to avoid losing access to Twitter, remove text-message two factor authentication by March 19, 2023."[8] Confusion about the steps that Twitter will take on this date only incentivise users to take the quickest action as soon as possible, which is to disable 2FA.

A simple search of "2FA" on Twitter supports this interpretation, as many users seem to consider Twitter's decision a complete elimination of 2FA for non-paying accounts, despite the other options still available. One user stated, "everyone's twitter account is going to get hacked now that they took 2FA away." The most recent statistics from Twitter's account security report also support this interpretation. The data reveals that in 2022, 2.6% of active users on Twitter had "at least one 2FA method enabled."[9] Of those users, 74.4% used the text messaging option.[10] Now that Twitter is taking away their most popular method of 2FA, it is very likely that those impacted will simply choose to disable 2FA either to avoid taking extra steps to set up other methods, or because those methods are slightly more inconvenient each time they log in. Whatever the reason, this decision by Twitter is compromising the security of those who don't pay for Twitter Blue.

Ironically, Twitter is representing this decision as *necessary* for the security of its users. In their announcement they state that "while historically a popular form of 2FA, unfortunately we have seen phone-number based 2FA be used - and abused - by bad actors. So starting today, we

---

[5] Solutions on the Digital Divide.
[6] Twitter Updated Policy at para. 4.
[7] *How to Use Two-Factor Authentication,* https://help.twitter.com/en/managing-your-account/two-factor-authentication (last visited Mar. 15, 2023).
[8] Dez Blanchfield, *"It's March Madness, #Twitter has now disabled 2FA via SMS.,"* (Mar. 9, 2023), https://twitter.com/dez_blanchfield/status/1634031967292497923.
[9] Twitter Inc., Account Security at § 2 (2022), https://transparency.twitter.com/en/reports/account-security.html#2021-jul-dec ("Account Security").
[10] *Id.*

will no longer allow accounts to enroll in the text message/SMS method of 2FA unless they are Twitter Blue subscribers."[11] According to the FTC, a deceptive act must "be a representation, omission or practice that is likely to mislead the consumer."[12] In this case, because users who pay still have access to text messaging 2FA, a consumer could reasonably interpret this statement to mean that Twitter Blue has extra security features that make text messaging 2FA safer than with a standard account. Therefore, consumers could be enticed to buy a subscription for security purposes, when in reality, text messaging 2FA has the same risks and benefits for either type of account.

Twitter is clearly misrepresenting this decision as an added security measure, when in reality it only serves to compel users to pay for Twitter Blue. Elon Musk amplified this misrepresentation when he tweeted: "Use of free authentication apps for 2FA will remain free and are much more secure than SMS."[13] He did not address the fact that this decision could cause many more people to disable 2FA or that users who pay for Twitter Blue will still have access to text messaging 2FA, both of which run contrary to claims of increased account security. Twitter understands how important 2FA is and has advocated for increased use in the past. In their 2022 account security report, Twitter stated that there is a "continued need to encourage broader adoption of 2FA, while also working to improve the ease with which accounts may use 2FA. Making 2FA methods simpler and more user friendly will help to encourage adoption and increase security on Twitter."[14] Taking away text messaging, the most user friendly option according to most in the industry, runs contrary to these aims and only serves to increase the company's profits off of Twitter Blue.

NHMC is highly concerned about the unfair and deceptive tactics Twitter has employed while implementing this new policy and its implications on the security of the platform. As you know, this is not the first time Twitter has misrepresented policies as benefitting security in an attempt to increase profits.[15] For that reason, we ask that the Commission ensure that Twitter is assessing and documenting this updated security practice in accordance with the 2011 Commission Decision and Order.[16] NHMC also applauds the steps that the Commission has

---

[11] Twitter Updated Policy at para. 2.
https://blog.twitter.com/en_us/topics/product/2023/an-update-on-two-factor-authentication-using-sms-on-twitter
[12] James C. Miller IIII, *FTC Policy Statement on Deception*, para. 4, (Oct. 14, 1983),
https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[13] Elon Musk, *"Use of free authentication…,"* (Feb. 18, 2023),
https://twitter.com/elonmusk/status/1627059645293670401.
[14] Account Security at § 2.
[15] Lesley Fair, *Twitter to Pay $150 Million Penalty for Allegedly Breaking Its Privacy Promises — Again* (May 25, 2022),
https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again.
[16] *In the Matter of Twitter, Inc., a corporation,* Docket No. C-4316, FTC Decision and Order, 202-3062, (2011),
https://www.ftc.gov/system/files/ftc_gov/pdf/ecf_11_stipulated_order.pdf.

taken recently to increase oversight of Twitter and urges you to consider this decision as a part of the ongoing investigation into Twitter's ability to protect users' privacy; weakening 2FA rather than actively encourage users to enable it will undoubtedly aggravate the privacy issues that already exist on the platform.

Thank you for your attention to this important issue. NHMC looks forward to addressing these harms in coordination with the Commission.

Sincerely,

Brenda Victoria Castillo
President & CEO
National Hispanic Media Coalition