STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, WC Docket No. 21-341 (September 30, 2021).

You may not know exactly how SIM swapping works, but you have probably heard about its harmful results. In 2019, hackers used a SIM swap to take control of Twitter CEO Jack Dorsey's singular twitter handle, @jack. In just 20 minutes, the hackers sent out two dozen tweets and retweets to @jack's millions of followers, including many toxic messages.[1] For Mr. Dorsey and his followers, the security breach caused alarm and offense. For other victims, there have been even more devastating consequences, from drained bank balances to lost email accounts containing years of communication.

SIM swapping and port-out fraud, a related scam, occur when a bad actor successfully poses as the victim in a transaction with the victim's phone company. The scammer can then take control of the Customer Proprietary Network Information associated with the victim's account, leverage that control to access bank accounts and other private information, and impersonate the victim in other harmful ways. These attacks are especially insidious because they are difficult for individuals—even those with all the security resources a large tech company can provide its senior leaders—to prevent on their own.

Protecting consumers from these kinds of scams will require systemic changes. I am pleased to support this Notice of Proposed Rulemaking because it begins the process of modernizing our CPNI and Local Number Portability rules to require carriers to act. I thank my colleagues for agreeing to two changes that I believe will make this NPRM even better. First, we have asked commenters to address the possibility of "future proofing" our guidelines for authenticating user identities by incorporating the National Institute of Standards and Technology's Digital Identity Guidelines or another authoritative source. As authentication technology improves and adapts to new threats, we will want our rules to keep up. Second, we will seek comment on whether and how the Commission should audit compliance with any carrier obligations we decide to adopt. There's good reason to think consumer complaints alone may not reliably surface problems like improper authentication procedures. After all, a consumer who calls her wireless company and gets the assistance she hoped for could be forgiven for not noticing if the customer service representative skips steps in the authentication process. I look forward to robust comments on these issues and the many other important questions raised in the NPRM, and I thank staff of the Wireline Competition Bureau for their hard work on this item.

[1] Brian Barrett, *How Twitter CEO Jack Dorsey's Account Was Hacked* (Aug. 30, 2019), https://www.wired.com/story/jack-dorsey-twitter-hacked/.