STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, WC Docket No. 21-34, Report and Order and Further Notice of Proposed Rulemaking (November 15, 2023).

It's a frightening thought – that a stranger could successfully impersonate you to your phone company, and in one conversation gain access to your primary means of communication. But this is more than a thought, it's reality. Bad actors are taking advantage of the services that let you keep your old number when you change phones or providers, leveraging identity authentication protocols and underdeveloped fraud response systems to, essentially, steal your phone and your account – without ever gaining physical control of it.

These scams – SIM swap and port-out fraud – don't just put wireless account access and details at risk. Because we so frequently use our phone numbers for two-factor authentication, a bad actor who takes control of a phone can also take control of financial accounts, social media accounts, the list goes on. Consumers must be able to count on secure verification procedures and reliable privacy guarantees from their wireless providers. And they should be able to go about their day without fearing that someone, somewhere, might take control of their phone without a single warning sign.

Today, we take action to provide that security. This order updates the Commission's existing Customer Proprietary Network Information ("CPNI") and Local Number Portability ("LNP") rules to protect against SIM swap and port-out fraud. While the framework we implement today is responsive to the current scope of these deceptive practices, it is also forward-looking. We require wireless providers to adopt secure authentication methods and to immediately notify customers of SIM change or port-out requests before they are processed, among other things. But we emphasize that these are baseline requirements, rather than prescriptive rules. In doing so, we acknowledge two things the record makes clear: first, that many providers may already have certain protective measures in place that may fulfill some of these new requirements, and second, that the threat landscape is rapidly evolving, and providers need flexibility to adopt and adapt their security methods accordingly.

Cell phones are near-ubiquitous, and many Americans rely on them as their sole means of connection, as well as the key to their many online accounts. The Commission's statutory duty to safeguard consumer privacy within the telecommunications space, and our unparalleled regulatory expertise within that space, gives rise to the strength of today's item. I thank the Chairwoman for her focus and leadership on these issues, and I thank the Commission staff for their excellent work on this item. It has my full support.