STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Protecting Consumers from SIM Swap and Port-Out Fraud*, WC Docket No. 21-341, Report and Order and Further Notice of Proposed Rulemaking (November 15, 2023).

If you want to know something about someone, just look at their phone. Because our phones do more than just connect us to friends and family. They are a record of where we have been and who we are. For many of us, these devices are internet gateways to our bank accounts, health records, social media profiles, and more. The convenience of accessing all of this through our phones is undeniable. But it also makes our devices a growing target for fraud—like SIM-swapping scams.

SIM cards are the dime-sized chips that are inserted into a mobile phone to identify and authenticate subscribers. When you want to upgrade your device, transferring your SIM card makes it easy to move your subscriber information to a new phone. But that's where fraudsters step in. A bad actor can call up your wireless provider and convince the customer service representative on the other end of the line that you really need to transfer your SIM card to a new device—a device that is in their control, not yours. If they are successful, they can divert two-factor authentication messages to drain your bank account, take over your social media profile, and hijack your e-mail.

The Federal Bureau of Investigation reports SIM-swapping scams are on the rise. But they are not alone. Because we see it here, too. At the Federal Communications Commission we are getting more and more complaints from consumers who have suffered losses due to SIM-swapping fraud. On top of this, the Cyber Safety Review Board at the Department of Homeland Security recently released a report investigating a bad actor responsible for extortion of a mix of companies and government agencies though SIM-swapping fraud. The report recommended that we take action to support consumer privacy and cut off these scams.

That is exactly what we do today. We require wireless carriers to give subscribers more control over their accounts and provide notice to consumers whenever there is a SIM transfer request, in order to protect against fraudulent requests made by bad actors. We also revise our customer proprietary network information and local number portability rules to make it harder for scam artists to make requests that get them access to your sensitive subscriber information.

We take these steps to improve consumer privacy and put an end to SIM scams. Because we know our phones know a lot about us. They are an entry to our records, our accounts, and so much that we value. That is why across the board we need policies that make sure our information is secure. It is also why I created the Commission's first-ever Privacy and Data Protection Task Force earlier this year. I want to thank them for their work on this initiative.

I also want to thank Allison Baker, Emily Caditz, Callie Coker, Adam Copeland, CJ Ferraro, Trent Harkrader, Melissa Kirkel, Chris Laughlin, Jodie May, and Jordan Reth from the Wireline Competition Bureau; Diane Burstein, Eliot Greenwald, Erica McMahon, Ike Ofobike, Suzy Rosen Singleton, Karen Schroeder, Kristi Thornton, and Kimberly Wild from the Consumer and Governmental Affairs Bureau; Loyaan Egal, Michael Epshteyn, James Graves, Phil Rosario, Kimbarly Taylor, Kristi Thompson, and Shana Yates from the Enforcement Bureau; Justin Cain, Ken Carlberg, Debra Jordan, Nicole McGinnis, Zenji Nakazawa, Erika Olsen, and Austin Randazzo from the Public Safety and Homeland Security Bureau; Garnet Hanly and Jennifer Salhus from the Wireless Telecommunications Bureau; Mark Azic, Patrick Brogan, Chelsea Fallon, Eugene Kiselev, Eric Ralph, and Emily Talaga from the Office of Economics and Analytics; Andrea Kearney, Doug Klein, Richard Mallen, and Derek Yeo from the Office of General Counsel; and Joycelyn James and Joy Ragsdale from the Office of Communications Business Opportunities.