Pillsbury Winthrop Shaw Pittman LLP
1200 Seventeenth Street, NW | Washington, DC 20036 | tel 202.663.8000 | fax 202.663.8007

Glenn S. Richards
tel 202.663.8215
glenn.richards@pillsburylaw.com

November 7, 2023

VIA ECFS

Marlene H. Dortch, Esq.
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: WC Docket No. 21-341 – Protecting Consumers from SIM Swap and Port-Out Fraud

Dear Ms. Dortch:

The Voice on the Net Coalition (VON) hereby submits a proposed change to the draft Report and Order released October 25, 2023, in the above referenced docket.[1] VON supports the Commission's efforts to protect consumers from malicious actors who seek to manipulate support agents and potentially compromise voice service accounts. The record demonstrates the need for robust safeguards to protect against bad actors that target customer support agents and use social engineering to gain unauthorized access to customer proprietary network information (CPNI).

VON recommends, however, that the Commission narrow the language of proposed new 64.2010(a) to ensure that customers continue to have the benefit of technical support, solutions engineers, customer success managers, and other staff that provide *outbound* technical and customer support. Doing so would be consistent with the Commission's careful efforts to ensure that its new requirements are not "overly prescriptive" or have "costs [that]

[1] Draft Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud (SIM Swap R&O),* WC Docket No. 21-341, FCC-CIRC2311-04 (October 25, 2023).

outweigh the benefits."[2] Solutions engineers, customer success managers, and staff in similar roles need access to CPNI to provide end users with the best communications experience possible, but their access does not present the same risks as customer support agents and others that receive *inbound* customer support requests. This is because it is *inbound* customer support that fraudsters can (and do) use to gain unauthorized access to sensitive customer information. Technical support and other support personnel that proactively reach out to customers, by contrast, need access to customer account information to provide technical support and solutions. Further, to the extent that these personnel have contact with end users, it is typically calls they place, which does not present the same risks as inbound customer contact; outbound customer contact will likely contacts provided by the customer, and is already subject to extensive consent and other regulatory requirements and, in any event, is not within the control of fraudsters and other bad actors.

Accordingly, VON recommends that the Commission modify the proposed language in new 64.2010(a) as shown below so that it clearly applies to those support agents that are more susceptible to the risks described in paragraph 50 of the draft Report & Order:

> "(a) Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit. **Telecommunications carriers shall establish safeguards and processes so that employees who ~~interact directly with~~ routinely receive inbound communications from customers, such as first-tier customer service agents, are unable to access CPNI until after a customer has been properly authenticated."**

Please direct any questions regarding this matter to the undersigned.

Respectfully submitted,

By: /s/
Glenn S. Richards
Counsel for VON

[2] SIM Swap R&O at para. 51.