Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	
	)	

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net Coalition (VON)[1] submits these comments in response to the Commission's Further Notice of Proposed Rulemaking asking whether new rules recently adopted to prevent wireless fraud should be applied to all telecommunications carriers and interconnected VoIP providers.[2] VON opposes any changes to the existing rules protecting customer proprietary network information (CPNI). There is no evidence in this proceeding that non-wireless customers are subject to the types of fraud the new rules are intended to address or that the existing CPNI rules are not working. Moreover, the Commission's recently adopted data breach rules will require all voice service providers to review and update their data protection practices and likely result in changes that will further secure customer information.

[1] The VON Coalition works to advance regulatory policies that enable Americans to take advantage of the promise and potential of IP-enabled communications. See www.von.org.
[2] *In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud,* Report and Order and Further Notice of Proposed Rulemaking *(SIM Swap Order and FNPRM),* WC Docket No. 21-341, (November 16, 2023); *see also* 88 Fed. Reg. 239 at p. 86614 (establishing a comment date of January 16, 2024). The FCC was closed on the January 16; thus the new deadline is January 17, 2024. See 47 CFR 1.4(e).

DISCUSSION

The *SIM Swap Order and FNPRM* does not raise any issues of relevance to interconnected VoIP providers. What it does address are two fraudulent practices that allow bad actors to take control of consumers' cell phone accounts – SIM swapping and port-out fraud. Specifically, the Commission revised its CPNI and Local Number Portability (LNP) "rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider."[3] The background section of the *SIM Swap Order and FNPRM* exhaustively reviews how bad actors access and swap SIMs, details the financial harms that can result from fraudulent SIM swaps, describes the increasing number of complaints filed with the FCC and FTC regarding the practice, and references an academic study that found vulnerabilities with the security practices of major wireless providers using insecure authentication challenges that could easily be subverted by bad actors requesting SIM changes.[4] The background section concludes with a brief history of the CPNI and LNP rules[5] and one paragraph summarizing the original notice of proposed rulemaking's intent to require wireless providers to adopt secure methods to prevent SIM swaps and porting fraud.[6] Similarly, the discussion and legal authority sections exclusively address

[3] *SIM Swap Order and FNPRM* at para. 2.
[4] *Id.* at paras. 4-10.
[5] *Id.* at paras. 11-16.
[6] *Id* at para. 17.

how wireless providers will implement the new rules, how those rules will protect wireless customers from SIM swaps and porting fraud and the legal authority for the Commission to impose the new rules on wireless carriers.[7]

The FNPRM asks whether the new SIM Swap fraud prevention rules should be "harmonized" with existing requirements governing customer access to CPNI and whether there would be any benefits from doing so (noting that similar questions were raised in the original notice of proposed rulemaking but the Commission did not act).[8] The Commission tentatively concludes, without any support or justification, that harmonized authentication requirements will be easier for wireless providers to implement and will be less confusing for customers. The Commission also provides no data regarding the number of incidents of unauthorized access to CPNI, including whether there have been any complaints or economic harm resulting regarding unauthorized access, or that the existing CPNI rules are not working.[9] More significantly, the FNPRM ignores the differences between the sensitivity and economic vulnerability of data

[7] *Id.* at paras. 18-97.

[8] *Id* at paras. 98-99. Comments filed in support of harmonization were predominantly from wireless carriers or carriers that offered wireless and other telecommunications services who would be subject to the new rules in any event. *Id.* at footnotes 344 and 345.

[9] The Commission should have at least attempted to provide anonymized, aggregated data collected from the CPNI breach reporting facility. See: Cpni Breach Reporting Facility | Federal Communications Commission (fcc.gov).

available from access to a wireless phone and the limited information available from access to CPNI.

The FNPRM also asks whether it would be costly and burdensome to adjust the CPNI authentication and protection practices they have already implemented.[10] Unequivocally yes. All customer support personnel will have to be retrained on the new procedures. In certain cases, third parties may provide customer support; thus change orders will have to be implemented. Compliance manuals will have to be rewritten. All of this takes time and requires human and financial resources that could be better used to develop better products and services.

The FNPRM also fails to address the new data breach rules released last month which expand the scope of the breach notification rules to cover not just CPNI but also personally identifiable information; expands the definition of breach to include inadvertent access, use or disclosure of customer information; requires notifications of breaches to the FCC and modified customer notice obligations.[11] These new rules will require all voice service providers to revisit their current data security practices and make the necessary changes to comply with the rules.

---

[10] *SIM Swap Order and FNPRM* at para. 101.

[11] *In the Matter of Data Breach Reporting Requirements,* Report and Order, WC Docket No. 22-21, FCC 23-111 (December 21, 2023). The new rules are scheduled to be effective 30 days after the order is published in the Federal Register, except for certain changes requiring approval from the Office of Management and Budget. See para. 155.

Before adopting more new rules, the Commission should allow companies time to comply and adapt to the expanded data breach reporting obligations.

The original CPNI rules were adopted in 1998 and have been subject to numerous updates in the 26 years that have passed since. While the rules provide a floor, nothing prevents covered service providers from implementing what they believe to be more secure practices. As a result of industry diligence, there have also been few reported cases of noncompliance by non-wireless providers in the past 15 years (indeed none are cited in the FNPRM). The Commission seeks to undo that success in six paragraphs in the FNPRM, in a proceeding focused on wireless fraud. In this case, the proposed rules are nothing more than a solution searching for a problem.

CONCLUSION

The Commission should act in accordance with the recommendations herein.

Respectfully submitted,

VOICE ON THE NET COALITION

/s/ *Glenn S. Richards*
Glenn S. Richards
Pillsbury Winthrop Shaw Pittman LLP
1200 Seventeenth Street, NW
Washington, DC 20036
(202) 663-8000

Its Attorney

January 17, 2024