Published on *The National Law Review* https://natlawreview.com

Shutting Down the Cell Phone Scammers: The FCC Adopts Rules to Crack Down on Fraudulent Practices against Wireless Phone Users

Article By:

Brian D. Weimer

Douglas A. "Drew" Svor

Elfin L. Noce

Ethan Lamb

On November 16, 2023, the Federal Communications Commission ("FCC") released a Report & Order ("Order") and Further Notice of Proposed Rulemaking ("FNPRM"), adopting measures to address two techniques bad actors frequently use to access victims' cell phone accounts: (1) SIM swapping and (2) port-out fraud.

Key Takeaway: To combat growing instances of SIM card and number porting fraud that expose wireless customers, the FCC is requiring wireless providers (including mobile virtual network operators, or "MVNOs") to implement customer authentication and other security methods to prevent these fraudulent practices.

Background

SIM swapping is a fraudulent practice where a bad actor impersonates a customer of a wireless provider in order to transfer

the victim’s mobile service to the bad actor’s device. Similarly, porting-out involves a bad actor requesting that a wireless provider transfer a victim’s phone number to a new wireless account controlled by the bad actor. When successful, both of these practices allow a bad actor to control the victim’s mobile account and exploit this access to customer proprietary network information (CPNI) and financial or social media accounts for fraudulent purposes.

New Framework: Updating the CPNI and LNP Regulations.

In order to protect consumers from these fraudulent practices, the FCC established a new baseline framework to combat SIM swapping and port-out fraud by updating its CPNI and local number portability (LNP) rules. The FCC rejected prescriptive requirements, instead focusing on baseline rules protecting against SIM swapping and port-out fraud while giving wireless providers flexibility to tailor their specific security measures.

Among other proposed regulations, the Order would require wireless providers to take the following actions:

Customer Authentication and Notification

- Use a secure method of authenticating customers prior to performing SIM changes (including both physical and virtual SIMs) and number ports;
- Review (at least annually) and update their customer authentication methods (as necessary);
- Notify consumers of SIM change and port-out requests and offer customers the option to lock their accounts to block processing of SIM changes and number ports, etc.; and
- Offer all customers, at no cost, the option to lock or freeze

their account to stop SIM changes or port-outs.

Internal Processes and Consumer Safeguards

- Implement a process for responding to failed authentication attempts in connection to a SIM change request;
- Establish processes to reasonably track and maintain information regarding SIM change requests and their authentication measures, and to retain that information for a minimum of three years;
- Establish safeguards and processes so that employees who receive inbound customer communications are unable to access CPNI in the course of that customer interaction until after a customer has been properly authenticated;
- Develop and implement training for employees on how to identify, investigate, prevent, and remediate SIM swap and port-out fraud; and
- Maintain a clear process for customers to report suspected fraud.

The Order will be effective 30 days after publication in the Federal Register, and compliance with the rules described above will be required six months after the effective date of the Order—with the exception of some rules (primarily, the rules requiring customer notification and internal security procedures) that will become effective on the later of six months or OMB approval.

Further Notice of Proposed Rulemaking.

The FNPRM seeks comment on whether to harmonize the existing requirements governing customer access to CPNI outside of the context of SIM changes with the new SIM change authentication and protection measures adopted in the Order. Comments on the FNPRM are due 30 days after the date of publication in the Federal

Register.

National Law Review, Volumess XIII, Number 334