FCC Proposes Amending Privacy and Number Portability Rules to Stop Virtual Cell Phone Theft

October 21, 2021

On September 30, 2021, the Federal Communications Commission ("FCC") adopted a Notice of Proposed Rulemaking ("NPRM") proposing new requirements for mobile wireless carriers to protect consumers from two practices that nefarious actors use to take control of a subscriber's cell phone service without gaining control of the subscriber's device. With "SIM swap fraud" a bad actor fraudulently convinces a carrier to transfer wireless services from a cell phone associated with a subscriber's subscriber identity module ("SIM") to a cell phone associated with another SIM and controlled by the bad actor. "Port-out fraud" is the practice of arranging for a phone number to be transferred from a subscriber's wireless carrier account to an account the bad actor has opened with another carrier. In both cases, the bad actor gains access to customer account information and can start sending and receiving calls and text messages using the victim's account or phone number, including text messages customers receive for two-factor authentication.

The Commission's consumer protection action arises from numerous complaints from consumers who have suffered harm as a result of these practices, and from concerns that consumers are vulnerable to these acts because wireless carriers have not implemented adequate protocols to verify that SIM swap and port-out fraud requests. To mitigate them, the agency suggests revisions to its Customer Proprietary Network Information ("CPNI") and Local Number Portability ("LNP") rules.

Proposed CPNI Rule Revisions to Combat SIM Swapping

Although narrowly-tailored, specifically covering the account information, call detail information, and billing information that voice service providers collect from their subscribers, the FCC's CPNI rules are among the most robust consumer privacy protections in the technology sector. The rules require voice providers to secure opt-in or opt-out consent for certain uses and disclosure of CPNI, to establish policies and procedures to discover and prevent unauthorized access to CPNI by third parties, to notify customers when certain account changes are made, and to notify law enforcement and customers when a breach of CPNI has occurred. Many of these rules were adopted or strengthened in 2007, when the FCC took action against another practice designed to gain unauthorized access known as "pretexting."

To reduce the incidence of SIM swap fraud, the NPRM proposes to modify the CPNI rules to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating the customer. As its primary proposal, the FCC puts forth four secure authentication methods that are already familiar to consumers: (1) a pre-established password; (2) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (3) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (4) a

passcode sent using a voice call to the account phone number or a preregistered back-up telephone number.

The FCC also offers two alternative approaches to give carriers flexibility to adopt new and better authentication methods as they are developed and in the event the proposed methods become less secure over time. First, the NPRM asks if the FCC should simply require carriers to adopt "heightened authentication measures" for SIM swap requests, which would allow them to choose from any secure authentication methods available at the time. Second, the NPRM asks whether the FCC should require carriers to comply with the NIST Digital Identity Guidelines, which provide technical requirements for federal agencies "implementing digital identity services" with a focus on authentication—these guidelines are updated regularly in response to changes in technology.

Beyond the authentication methods, the NPRM also seeks comment on other protections to prevent unauthorized SIM swaps. For example, it asks what procedures carriers should be required to adopt in the event there are several failed authentication attempts, whether customers should be notified of requests for SIM changes, and whether SIM swaps should be delayed pending notification or verification from the affected customer. It also suggests that customers be able to disable SIM changes by phone or online and that customers be notified of SIM swap protection methods annually. In addition, the NPRM asks whether the FCC should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud.

Proposed LNP Rule Revisions to Combat Port-Out Fraud

The FCC's LNP rules allow consumers to retain their phone numbers when switching telecommunications service providers by requiring providers to port phone numbers to a customer's new carrier upon request. While the FCC has codified requirements for providers to validate requests for wireline-to-wireline and intermodal porting, it has only provided guidance for wireless-to-wireless requests based on common industry practices. Specifically, for wireless-to-wireless port-out requests, the guidance suggests that providers validate requests using telephone number, account number, and ZIP code, as well as a customer passcode, if established by the customer.

In proposing rules to prevent port-out fraud, the FCC is seeking to balance the need to protect consumers from the fraudulent practice with its goals under the LNP rules—namely, ensuring that port-out requests are processed and done so in a timely manner, thereby promoting competition among providers by enabling consumers to choose a carrier that best suits their needs. In striking this balance, the NPRM proposes to modify the LNP rules to require that wireless carriers notify customers through a text message or push notification when a port-out request is received so that customers can take steps to stop unauthorized requests. But it also asks if the FCC should go a step further and require customer verification or acknowledgement of the notification.

The NPRM also asks for comment on several additional items to prevent port-out fraud. For instance, it asks whether other methods currently used by providers are effective in preventing the practice and should be imposed on other carriers. It also proposes codifying the four types of information carriers must use to validate wireless-to-wireless port-out requests. Finally, the NPRM asks what, if any, effect its proposed rules would have on timing of port-out requests and competition.

Wireless providers who are interested in informing the FCC's decisions regarding changes to its CPNI and LPN rules can file initial comments on November 15, 2021 and reply comments on December 14, 2021.