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

FCC Acts to Protect Consumer Data by Strengthening Customer Proprietary Network Information and Number Porting Rules

Article By:

Eduardo R. Guzmán

Paul C. Besozzi

The Federal Communications Commission ("FCC") has adopted rules to address two fraudulent practices that "bad actors use to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of the consumer's phone."

In its recent Report and Order and Further Notice of Proposed Rulemaking released November 16, 2023, the Commission first addressed the practice where bad actors are able to swap a consumer's subscriber identity module ("SIM") card to a wireless device associated with a different SIM (i.e., SIM card swap fraud). The agency also acted on wireless number porting fraud, where bad actors impersonate a customer and convince the provider to port the real customer's telephone number to a new wireless provider and a device that the bad actor controls (i.e., port-out fraud).

The FCC noted that in both cases the bad actor "has acquired the means to take control of many more of the victim's accounts, which can result in substantial harm to the customer." This could include the interception of "text messages and phone calls used to authenticate a customer's financial, social media and other accounts." The fraud may provide the means for the bad actor to "gain access to these accounts and then change

login credentials, obtain sensitive information, drain bank accounts and sell or try to ransom social media accounts." These abuses are successful even in the face of information used by wireless providers to authenticate their customers.

To prevent these instances of fraud the FCC has amended its rules relating to (i) individual customer proprietary network information ("CPNI"), which primarily reflects the customer's telephone usage, and (ii) number portability, which, for example, allows a consumer to "port" a cell number from one provider to another. The FCC sets baseline rules that are intended "to establish a unform framework across the mobile wireless Prior to conducting a SIM change industry for the types of policies and procedures providers must employ to combat SIM swap and port-out fraud."

SIM Swap Fraud – Under amended CPNI rules, wireless providers will now be required to do the following to combat SIM swap fraud:

- Prior to implementing a SIM change, use secure methods to authenticate a customer that are reasonably designed to confirm a customer's identity, except otherwise required in domestic violence and other circumstances under the Safe Connections Act and its implementing rules. Providers must not less than annually review and update as necessary their customer authentication methods.
- Develop, maintain, and implement procedures for responding to failed authentication attempts in connection with a SIM change request that are reasonably designed to prevent unauthorized access to the customer's account, taking into consideration requirements of the Safe Connections Act and its implementing rules.
- Provide immediate notification to customers of any requests for a SIM change associated with their account, before any SIM change is made, again subject to the requirements of the Safe Connections Act and its implementing rules.
- Offer all customers, at no cost, the option to lock or freeze their account to stop SIM changes. Providers are permitted to proactively initiate a SIM swap lock on a customer's account when a provider believes the customer may be at a high risk of fraud.
- Establish processes to reasonably track and maintain information

regarding SIM change requests and their authentication measures, and retain the information for at least 3 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 the customer has been properly authenticated.

Port-Out Fraud – The Commission adopts similar requirements relating to:

- authentication of customers,
- notification of customers of port-out attempts, and
- options to lock or freeze their accounts from port outs.

Other consumer protection measures directed by the Commission to address these fraudulent practices are:

- Notification to customers of account protection measures.
- Training employees on how to identify, investigate, prevent as remediate SIM swap and port-out fraud.
- Maintaining a clearly disclosed, transparent, and easy to use process for customers to report SIM swap and port-out fraud, promptly investigate the same, and provide customers documentation regarding such fraud on their accounts.

Implementation Timeframe – Wireless providers must comply with these requirements six months after the effective date of the Order, which will be 30 days after publication in the Federal Register, or, for those requirements subject to review by the Office of Management and Budget, upon completion of that review, whichever is later.

Further Notice of Proposed Rulemaking – Finally, the FCC seeks further comment on:

- harmonizing standards and government efforts to combat these fraudulent activities, and
- requiring customer notification of failed customer authentication attempts.

National Law Review, Volumess XIII, Number 335