

# Congress of the United States

Washington, DC 20510

January 9, 2020

The Honorable Ajit Pai  
Chairman  
Federal Communications Commission  
445 12th Street Southwest  
Washington, D.C. 20554

Dear Chairman Pai:

We write to urge the Federal Communications Commission (FCC) to require wireless carriers to protect consumers from fraud and the theft of their most sensitive personal data by criminals and foreign governments who can empty their bank accounts, read their personal email and access their private photos and documents.

Consumers are regularly advised by companies, government agencies and experts to secure their critical online services using two-factor authentication. These services often use text messages (SMS) as their second factor. But fraudsters are often able to get wireless carriers to transfer the cell phone accounts of victims to them, steal their login credentials and then empty their victims' bank accounts. This method of fraud is known as "SIM swap" fraud. The impact of this type of fraud is large and rising. According to the Federal Trade Commission, the number of complaints about SIM swaps has increased dramatically, from 215 in 2016 to 728 through November 2019, and consumer complaints usually only reflect a small fraction of the actual number of incidents. Moreover, according to the Wall Street Journal, "Investigators with the Regional Enforcement Allied Computer Team, a law-enforcement task force in Santa Clara County, said they know of more than 3,000 victims, accounting for \$70 million in losses nationwide."

SIM swap fraud may also endanger national security. For example, if a cyber criminal or foreign government uses a SIM swap to hack into the email account of a local public safety official, they could then leverage that access to issue emergency alerts using the federal alert and warning system operated by the Federal Emergency Management Agency. Countless other U.S. government websites used by millions of Americans either allow password resets via email or support two-factor authentication via SMS, which can both be exploited by hackers using SIM swaps.

Consumers have limited options to protect their wireless accounts from SIM swaps and are often not informed about these options by carriers until after they have been victimized. In some cases, the SIM swaps have been facilitated by corrupt employees working for the phone company. For example, in May of 2019, the Department of Justice indicted several people who had exploited their employee access to the carriers' computers to conduct SIM swaps that defrauded victims of more than \$2 million. Consumers have no choice but to rely on phone companies to protect them against SIM swaps — and they need to be able to count on the FCC to hold mobile carriers accountable when they fail to secure their systems and thus harm consumers.

According to press reports, some carriers, both in the U.S. and abroad, have adopted policies that better protect consumers from SIM swaps, such as allowing customers to add optional security protections to their account that prevent SIM swaps unless the customer visits a store and shows ID. Other carriers will only conduct SIM swaps after confirming the receipt by the customer of a one-time password sent by email or text message. Carriers in other countries, including Nigeria, South Africa, Kenya, the United Kingdom and Australia, also make SIM swap data available to financial institutions so that they can take appropriate additional security measures if a customer's SIM has been swapped recently.

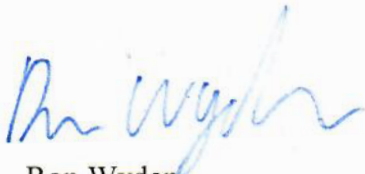
Unfortunately, implementation of these additional security measures by wireless carriers in the U.S. is still spotty and consumers are unlikely to find out about the availability of these obscure, optional security features until it is too late. As the primary regulator of the wireless industry, the FCC has the responsibility and authority to secure America's communication networks and protect consumers who rely on those networks. To that end, we urge the FCC to initiate a rulemaking to protect consumers from SIM swaps, port outs and other similar methods of account fraud. Please also provide us with answers to the following questions by February 14, 2020:

1. Does the FCC track incidents of SIM swapping or port-out fraud, e.g., through its consumer complaints system? If so, how many reports has the FCC received in each of the last thirty-six months?
2. Criminals use port outs to move numbers to their own service with a different carrier. Do you believe that the current number porting rules (e.g., 47 CFR § 52, the North American Numbering Council recommendations or the LNPA WG Local Number Portability Best Practices) or the rules for Changes in Preferred Telecommunications Service Providers (47 CFR § 64.1100 et seq., "anti-slamming" rules) are sufficient to prevent fraudulent ports?
3. Criminals can use SIM swapping to access the historical call records of their victims, as the carrier online account web sites often rely on SMS for password recovery. Does the FCC believe that the carriers' legal obligation to secure their customers' call records under 47 USC § 222 extends to protecting customer online accounts from this form of hacking?
4. Does the FCC provide consumers with information on steps they can take to reduce the risk of becoming a victim of illegal SIM swapping. If not, why not?
5. In other countries, banks can obtain the most recent SIM swap date of a customer from their carrier to flag potentially suspicious log-in attempts. Does the Commission consider SIM activation dates to be customer proprietary network information or otherwise restrict carriers from providing this information to third parties with the customer's permission?
6. Do the FCC's CPNI rules prevent mobile carriers from reporting illegal SIM swaps to law enforcement authorities?
7. Has the FCC received reports of violations of CPNI involving the hacking of the wireless carriers, including computers in retail stores and those used by customer service agents?

8. Has the FCC initiated investigations or taken enforcement actions related to these reports?

Thank you for your attention to this serious matter.

Sincerely,



Ron Wyden  
United States Senator



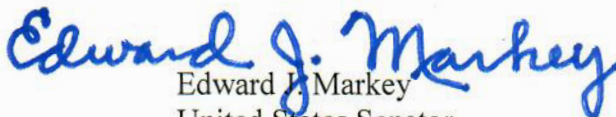
Ted W. Lieu  
United States Representative



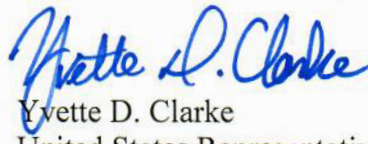
Sherrod Brown  
United States Senator



Anna G. Eshoo  
United States Representative



Edward J. Markey  
United States Senator



Yvette D. Clarke  
United States Representative

Cc: The Honorable Michael O'Rielly, Commissioner  
The Honorable Brendan Carr, Commissioner  
The Honorable Jessica Rosenworcel, Commissioner  
The Honorable Geoffrey Starks, Commissioner