An Open Letter to Ajit Pai, Chairman of the FCC

By Michael Terpin, 25+ year mobile carrier customer and SIM Swap victim

Chairman Pai:

Today, the mobile communications industry is among the largest, most powerful and fastest growing industries in the history of mankind. From its humble roots in the 1980s, offering the elite consumer expensive "brick" and non-portable "car phones," the industry has grown to its current worldwide ubiquity, with more than 5 billion users and nearly 9 billion mobile connections (more than one per every person on earth), according to GSMA Intelligence.

With that rapid growth has come both massive innovation and improvements in the user experience, including bringing real-time communication to some of the poorest areas of the world, which never previously built out reliable landline services. Yet, with this growth and incredible prosperity (the market caps of "big four" carriers in the US alone exceed $625 billion) has come a responsibility to the consumers that your Commission exists to protect.

I have watched over the years as the FCC has made many laudable decisions on behalf of consumers, including protection from telemarketers; data portability; and just in the past few months a new push to combat robocalls, which you called a "scourge" and "a top priority" for the FCC. Indeed, there are more than 200 articles on the FCC website mentioning robocalls – and yet not one addressing the fastest growing cancer on the mobile consumer landscape: the hacking of personal information, accounts, identity theft and money via a growing crime called "SIM swapping" or "simjacking."

The theft of a consumer's SIM (subscriber identity module) is tied to much more than just the ability to send and receive phone calls and texts to the correct device. Since the mobile industry encouraged software providers to use SMS texts as a second factor of authentication (also known as 2FA) for everything from email and social networks to application software and financial services accounts, as well as enabled wireless transfer of SIM ownership to new devices, it has emboldened a pernicious new wave of organized crime: SIM swappers.

Twitter CEO Jack Dorsey's SIM swapping, which enabled a group of hackers to take over his identity on Twitter and post racist tweets, was the most high-profile case of SIM swapping, but far from the most damaging. In the blockchain and cryptocurrency world, where I have been working as an investor, advisor and marketer since 2013, there have been hundreds of millions of dollars of hacks of cryptocurrency, including exchanges, where the hack was enabled by the ease of stealing a key executive or investor's digital identity and authority via this crime.

In general, SIM swaps are orchestrated by highly sophisticated, repeat offender, criminal gangs (some of which are finally being arrested and in one case so far, convicted and sentenced). An entire new task force (REACT) was set up last year by Homeland Security and the Santa Clara County Sheriff's Department to help investigate these crimes (the FBI and other agencies also have their fair share of cases, including mine, which I will summarize below).

On January 7, 2018, after having obtained "high security" protection on the two carriers I used (AT&T and T-Mobile) following a prior, smaller SIM swap seven months earlier, as well as spending weeks with the industry's top security professionals to add even more protection to my assets, I was hit again by a criminal gang on my AT&T account (my T-Mobile account, whose high-security provision included a "no port" directive, was unaffected; AT&T does not offer a "do not port" option to consumers). We contend the hack began with an AT&T representative in a Connecticut retail store turning over my credentials to the gang, resulted in the loss of $24 million.

I am not alone, of course. The REACT Task Force has taken on hundreds of cases (including new ones every month I refer to them; since I announced my lawsuit, I have been contacted by more than 50 individuals who experienced similar hacks, with losses in a few instances of more than $10 million). On Friday, another investor sued AT&T for the $1.8 million taken from him in a similar SIM Swap during the May 2018 Consensus conference. In his case, the AT&T representative who sold his information to a criminal gang has already been arrested by Homeland Security for this theft and 40 others; one of his hackers has been arrested and convicted.

Chairman Pai, you and the FCC have the unique opportunity and authority to end this scourge quickly and effectively by taking three actions:

1) Mandate that all US mobile carriers cover their PINS and passwords, so that users must punch them in instead of reading them aloud to a retail clerk or call center employee. Banks, hotel chains and airlines cover their passwords. The vital data and access protected by these four- to six-digit PINS is too valuable to trust the screening out of potential criminals from tens of thousands of employees and agents. Let the technology do the work and protect all consumers.

2) Inform all US mobile carrier customers that they can opt-in to carrier high-security plans (all carriers have these, but they don't inform customers at the time of purchase, as they do with insurance against damaged devices). These high-security plans must include a "no port" option, whereby a consumer can specify that his phone cannot be ported without going through the fraud department. This would be similar to how credit card companies protect their consumers.

3) Initiate an immediate, comprehensive study (as was done for robocalls) with recommendations for mandatory reforms by the carriers.

These first two measures are easy to implement: the first would simply require using a phone keypad to punch in the numbers, something every carrier already uses for other commands, and the second would mandate a policy that some, but not all, carriers already offer.

Chairman Pai, I will be attending your opening keynote at Mobile World Congress Americas in Los Angeles on Tuesday (I'm a speaker myself on Thursday, addressing how carriers can add user value and make considerable revenue by integrating blockchain technology into its current offerings). I look forward to the opportunity to address this with you and your fellow commissioners.

Sincerely,

Michael Terpin
michael@transformgroup.com
+1 (646) 926-6420

cc: Meredith Attwell Baker, president and CEO, CTIA