PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 15, 2021

Federal Communications Commission
45 L Street NE
Washington, DC 20554

COMMENTS IN THE MATTER OF PROTECTING CONSUMERS FROM SIM SWAP AND PORT-OUT FRAUD
WC Docket No. 21-341

Thank you for the opportunity to provide comments on how the FCC can protect telecommunications customers from subscriber identity module (SIM) swap fraud, number port-out fraud, and related security and privacy threats.

We are academic researchers affiliated with the Center for Information Technology Policy (CITP) at Princeton University, one of whom previously served as Chief Technologist of the Commission's Enforcement Bureau. In a recent computer science publication, which the Commission references in the Notice of Proposed Rulemaking, we examined the SIM swap customer authentication practices of major U.S. wireless carriers.[1]

Our study involved a straightforward methodology. We created ten prepaid accounts at each of five carriers, then called customer service and attempted a SIM swap using limited information that might be available to an unsophisticated attacker. Our research methods enabled us to document the customer authentication process for each carrier.

We found pervasive insecurity. All five carriers used forms of customer authentication that are not generally accepted in the field of information security and that have serious security shortcomings. Carriers also did not have an apparent mechanism for responding to suspicious or failed authentication attempts—we were able to keep trying alternative modes of authentication, without notice to our simulated account owners. On several occasions, customer service representatives volunteered account information even though we had not successfully authenticated.

[1] Kevin Lee, Benjamin Kaiser, Jonathan Mayer & Arvind Narayanan, *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, Usenix Symposium on Usable Security and Privacy (Aug. 2020), *available at* https://www.usenix.org/system/files/soups2020-lee.pdf (attached as a copy for purposes of the rulemaking record).

We offer the following recommendations for refining and strengthening the Commission's proposed rules, based on our recent research and experience in the field of information security.

1. **The Commission should set a baseline of strong customer authentication for SIM swaps.**

We support the Commission's proposal to require that carriers complete strong customer authentication before effectuating a SIM swap. We offer several recommendations for how the Commission might improve on its proposal.

   a. **We recommend refining the enumerated methods of permissible authentication.**

The Commission identifies four methods of authentication that would be sufficient for effectuating SIM swaps: passwords, passcodes via email, passcodes via SMS, and passcodes via voice calls.

We support the inclusion of passwords as a recognized method of authentication. Passwords, which demonstrate that the authenticating customer possesses secret knowledge, have been a cornerstone of information security for decades. But the type of password matters: short and easily guessable passwords provide limited security.[2] We recommend that the Commission clarify that, if a carrier relies on passwords for customer authentication, it must implement passwords consistent with current best practices (e.g., Section 5.1.1 of NIST Special Publication 800-63B). We additionally recommend that the Commission require carriers to regularly check customer passwords against datasets of widely used and compromised credentials, to protect customers from both targeted and large-scale ("credential stuffing") password guessing attacks.

We are neutral on the inclusion of passcodes via email, which effectively delegate authentication to a customer's email provider.[3] This type of authentication can be secure, when the customer's email provider uses strong authentication itself and when

[2] *See, e.g.*, Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin & Lorrie Faith Cranor, *"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab*, Usenix Symposium on Usable Security and Privacy (July 2015), *available at* https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ur.pdf

[3] We use the term "passcode" because it appears in the Commission's proposed rules, but if the Commission allows customer authentication via email or telephone, we recommend clarifying that sending a non-numeric password or an authentication link is also permissible.

the email traffic between the carrier and the customer's email provider is protected by modern security standards that include cryptographic authentication.[4] Those assumptions do not always hold, though, and the level of confidence provided by email authentication is less than that provided by methods of authentication linked to a specific device (see Section 5.1.3.1 of NIST Special Publication 800-63B). We believe that, on balance, the familiarity and usability of emailed passcodes may justify their inclusion as a permissible form of authentication. But we also believe it would be reasonable to omit emailed passcodes as a permissible method of authentication.

We also have reservations about the Commission's proposed inclusion of passcodes via SMS and voice calls as permissible methods of authentication. The public switched telephone network (PSTN) has known call and SMS routing vulnerabilities, and criminals have previously exploited those vulnerabilities.[5] We agree with NIST's determination that PSTN-based authentication poses much greater security risks than methods of authentication that prove a customer possesses a specific device.

We encourage the Commission to delineate between two types of telephone-based authentication, which have very different security properties: authentication using the carrier's own network, and authentication using the PSTN. We support allowing SMS and voice call authentication methods when the carrier can deliver the passcode exclusively over its own network and to a specific known device (e.g., smartphone) or point of service (e.g., landline phone) connected to the network and controlled by the customer. In these scenarios, a carrier can have confidence that the passcode was not maliciously rerouted over the PSTN.

We recommend against permitting SMS and voice passcodes over the PSTN, because these authentication methods are less secure. But, as with emailed passcodes, we believe the Commission could reasonably weigh the security and usability considerations and arrive at either outcome.

---

[4] *See* Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicolas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey & J. Alex Halderman, *Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security*, IMC '15: Proceedings of the 2015 Internet Measurement Conference (Oct. 2015), *available at* https://doi.org/10.1145/2815675.2815695; Hang Hu & Gang Wang, *End-to-End Measurements of Email Spoofing Attacks*, USENIX Security Symposium (Aug. 2018), available at https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-hu.pdf.

[5] *See* Russell Brandom, *For $500, This Site Promises the Power to Track a Phone and Intercept Its Texts*, The Verge (June 13, 2017), *available at* https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime; Russell Brandom, *This Is Why You Shouldn't Use Texts for Two-factor Authentication*, The Verge (Sept. 18, 2017), *available at* https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin.

If the Commission permits emailed passcodes or passcodes over the PSTN, we recommend several additional safeguards for those methods of authentication. First, any email, call, or SMS containing a passcode should include a clear and conspicuous warning not to share the passcode with third parties. Attackers can be successful at tricking victims into forwarding these passcodes, enabling account compromise to occur. Second, Commission staff should periodically revisit the security of these authentication methods and reevaluate whether to retain them. Third, if NIST concludes that PSTN-based authentication should be downgraded further in its Digital Identity Guidelines (e.g., from RESTRICTED to DEPRECATED), the Commission's rules should automatically phase out those methods of authentication.

b. We recommend specifying the security properties of alternative methods for authentication.

In the proposed rules for SIM swap authentication, the Commission provides that the four enumerated methods "shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication." We strongly agree that the Commission's customer authentication rules should not be technically prescriptive. Authentication methods and security practices continue to evolve, and carriers should be welcome—and encouraged—to adopt innovative safeguards. What matters are authentication security *properties*, not the specific technical means that carriers use to *implement* those properties.[6]

As currently drafted, we do not believe the regulatory text provides sufficient guidance about what constitutes a "secure method of authentication." The term "secure" lacks specificity and is open to subjective interpretation. A carrier could, for example, take the position that questions about biographical information are "secure" because they remain in widespread use for online services.

We recommend that the Commission specify the properties that an authentication method must have for it to be considered adequately secure. In particular, we recommend that the Commission track NIST's approach: an alternative authentication method must at minimum prove that the customer *possesses* something.[7] That could be a

[6] As a point of comparison, the recent FTC authentication rules for financial services *exclusively* describe security properties and do not identify specific methods of authentication. We would support the Commission paralleling the FTC's approach.

[7] If the Commission addresses multi-factor authentication, which we discuss below, we further recommend permitting biometric authentication factors as secondary authentication factors. We agree

backup code issued by the carrier, a stored secret value (e.g., software that generates one-time codes), or a device (e.g., an enrolled smartphone app that delivers push notifications or a USB security key).

We note that this recommendation, combined with our prior recommendation for the enumerated methods of authentication, is substantively equivalent to Authenticator Assurance Level 1 of the NIST Digital Identity Guidelines with just two modifications. First, we are neutral about adding emailed passcodes as a permissible method of authentication. Second, our recommendations would require checking passwords against datasets of widely used and compromised passwords. We support including the NIST Digital Identity Guidelines by reference to make this substantive connection explicit.

c. We recommend requiring that carriers protect all customers with multi-factor authentication, or at minimum, make multi-factor authentication the default for all customers.

Multi-factor authentication (MFA) is an invaluable defense against customer account compromise. In a recent large-scale study of real-world logins and account compromise attempts, Google found that prompting for an additional authentication method protects customers from the overwhelming majority of bulk and targeted account compromises.[8] Many online services now require MFA, and the Federal Trade Commission recently promulgated Gramm-Leach-Bliley Act rules that require MFA for customers accessing financial services (including those offered by carriers).[9] Some services take a step short of mandating MFA, making it the default for new customers and either automatically enrolling existing customers or encouraging them to enable

---

with NIST's conclusion that, at this time, biometric systems are generally not secure enough to serve as exclusive authentication mechanisms (see Section 5.2.3 of NIST Special Publication 800-63B).

[8] Periwinkle Doerfler et al., *Evaluating Login Challenges as a Defense Against Account Takeover, World Wide Web Conference* (May 2019), *available at* https://research.google/pubs/pub48119/.

[9] Federal Trade Commission, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial.

MFA.[10] Earlier this year, for example, Google announced that it is automatically enabling MFA for over 150 million accounts.[11]

We recommend requiring that carriers protect all customers with MFA. MFA will be a familiar experience for the vast majority of telecommunications customers because it has now been so widely deployed by online services—especially in other areas of critical infrastructure that Americans depend on (e.g., healthcare and finance).[12] MFA also poses a particularly modest burden in the telecommunications sector, because many customers will not have reason to log into an account more than monthly to pay their bill (and even less often with autopay). For almost all customers, the security benefits of MFA will far outweigh the modest burden.

That said, the record for this proceeding may reveal that there are telecommunications customers who have difficulty with MFA. If the developed record includes specific evidence that there are customers who are significantly disadvantaged by implementing MFA, we recommend that the Commission establish—at minimum—a default of MFA for new and existing customers. If the Commission chooses this approach, we recommend requiring that carriers clearly communicate to customers that opting out of MFA places their account at greater risk of compromise.

d. We recommend refining the Commission's proposal requiring procedures for responding to failed account authentication attempts.

In our recent study of wireless carrier customer authentication, we found that carriers did not implement adequate safeguards for preventing an attacker from repeatedly calling customer service and attempting a SIM swap. We saw no evident response from carriers to our suspicious customer authentication attempts.

We support the Commission's proposal requiring that carriers implement procedures for responding to failed account authentication attempts, and we offer two improvements to the proposal. First, we recommend that the Commission require that

---

[10] *See* Katie Deighton, *Tech Companies Push Users to Adopt Two-Factor Authentication*, The Wall Street Journal (Nov. 1, 2021), *available at* https://www.wsj.com/articles/tech-companies-push-users-to-adopt-two-factor-authentication-11635807088.

[11] AbdelKarim Mardini & Guemmy Kim, *Making Sign-in Safer and More Convenient*, Google Keyword Blog (Oct. 5, 2021), *available at* https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/.

[12] *See* Dave Childers, *State of the Auth Report*, Duo Labs Report (Sept. 14, 2021), *available at* https://duo.com/assets/ebooks/state-of-the-auth-2021.pdf.

the procedures be reasonably designed to prevent unauthorized access to a customer's account. The mere existence of *some* procedures for responding to repeated authentication failures should not be sufficient—for example, it should not be sufficient for a carrier to allow its customer service representatives, at their subjective discretion, to flag a SIM swap request as questionable.

Second, we recommend that rate limiting be required as a component of a carrier's procedures for responding to failed account authentication attempts. We do not see a need to be prescriptive about the specific rate limit (e.g., 3 attempts every 24 hours) so long as a carrier reasonably determines that the rate limit is low enough to prevent typical repeated attacks from succeeding.

e. We support the Commission's proposal requiring customer notification for SIM swap attempts.

Another issue we identified in our recent study was that carriers did not notify customers about SIM swap attempts. That notice is essential, so that a customer can take prompt action to protect their telecommunications account (e.g., updating a compromised password), their other accounts (e.g., stopping a fraudulent payment), and their devices (e.g., removing malware from a compromised device). In many SIM swap attacks, time is of the essence—an adversary's goal is to rapidly clear the victim's financial accounts, before the victim can respond.[13] We support the Commission's proposal requiring carriers to notify customers about SIM swap attempts, successful or not. We also recommend that the Commission clarify the baseline means of notice: a carrier should at minimum contact the telephone number and email address associated with the account. There is an unambiguous and material security upside to the Commission's proposal, and the only downside is a very infrequent notification that the customer can easily discard.

2. We recommend that the Commission require a carrier to authenticate a customer before a customer service representative can access the customer's account.

There is no reason for a customer service representative who is responding to a customer inquiry to have access to that customer's account before the customer has successfully authenticated. At best, providing that access is an unnecessary exposure of

[13] *See, e.g.*, Donie O'Sullivan, *One Man Lost His Life Savings in a SIM Hack. Here's How You Can Try to Protect Yourself*, CNN (Mar. 13, 2020), *available at* https://www.cnn.com/2020/03/13/tech/sim-hack-million-dollars/index.html.

customer data and a violation of the information security principle of minimizing system permissions (sometimes referred to as the "principle of least privilege"). At worst, this practice invites adversaries to exploit sympathetic, inattentive, or malicious customer service representatives for account access. There should be no opportunity for a representative to give a hint or a free pass—the authentication process should be identical no matter which representative answers.

We recommend a straightforward fix. Until a customer has successfully authenticated with the carrier, a customer service representative responding to an inquiry should be completely prohibited from that customer's account—no access to data and no ability to make changes. If a customer encounters difficulty authenticating, the solution should be backup methods of authentication (which we discuss shortly).

3. **The Commission should modernize and harmonize baseline authentication requirements for telephone access to CPNI, online access to CPNI, SIM swaps, and number portability authentication methods.**

The Commission's proposed rules would establish five separate customer authentication standards: (1) telephone access to CPNI, (2) online access to CPNI, (3) in-store access to CPNI, (4) SIM swaps, and (5) number portability. We recommend that the Commission take this opportunity to generally modernize and harmonize its baseline authentication requirements.[14]

First, we believe that a unified approach provides the appropriate level of protection for customer data and connectivity. CPNI can be extraordinarily sensitive, as the Commission and Congress have previously acknowledged.[15] Port-out frauds can also be just as harmful as SIM swap frauds.[16] Rather than creating a new heightened level of authentication for SIM swaps and a different heightened level of authentication for

[14] We call the Commission's attention to the recent Federal Trade Commission rulemaking on authentication for financial services (including certain services provided to customers by carriers), which may provide a helpful template for modernized and harmonized authentication requirements.

[15] We also encourage the Commission to consider extending the customer authentication rules to "customer proprietary information" under 47 U.S.C. § 222(a), such that the rules unambiguously apply to all aspects of a telecommunications customer's account.

[16] While we do not take a position on how to integrate strong customer authentication into number portability, one straightforward near-term approach would be to require that the port-out carrier complete strong customer authentication before issuing a passcode and that the port-in carrier submit the passcode for validation. The Domain Name System (DNS) relies on a similar authentication mechanism for porting domain names between registrars, and the Commission may find it helpful to examine DNS customer authentication in updating its rules.

port-outs, we recommend that the Commission raise the baseline level of authentication for all customer access to account data and changes to account settings.[17]

Second, a unified approach would prevent inconsistencies in the strength of authentication depending on how a customer happens to contact a carrier.[18] As we previously noted, customer service representatives are a potential point of authentication vulnerability and should not be able to provide hints about or bypass customer authentication. Similarly, an in-person customer service representative should not be able to simply assert that they have validated a customer's photo identification and gain access to the customer's account. There have been multiple instances of carrier employees abusing insider access to facilitate SIM swap frauds, and criminal organizations make concerted efforts to recruit carrier employees to participate in fraud schemes.[19] The security of customer records and connectivity should not depend on the

---

[17] Carriers should, of course, remain welcome to implement *additional* customer authentication safeguards. Those additional safeguards could also vary by the sensitivity of the customer's request. Our recommendation is that the Commission modernize and harmonize *baseline* authentication requirements.

[18] There are a range of technical designs for linking strong authentication to a telephone or in-person customer service conversation. A customer could, for example, log into the carrier's website or mobile app and then affirmatively approve of the customer service session. An even stronger approach would be to uniquely identify the customer service session (e.g., with a passcode) during approval. We do not take a position on how carriers link "out-of-band" strong customer authentication to customer service sessions, so long as the methods are reasonably secure and warn customers of the risks from approving an unauthorized customer service session.

[19] *See* U.S. Department of Justice, Office of the U.S. Attorneys, Eastern District of Michigan, *Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges*, May 9, 2019, https://www.justice.gov/usao-edmi/pr/nine-individuals-connected-hacking-group-charged-online-identity-theft-and-other; U.S. Department of Justice, Office of the U.S. Attorneys, Eastern District of Louisiana, *California Resident Charged in Superseding Indictment for Role in Sim Swap Scam Targeting at Least 40 People, Including New Orleans Resident*, Sept. 13, 2021, https://www.justice.gov/usao-edla/pr/california-resident-charged-superseding-indictment-role-sim-swap-scam-targeting-least; U.S. Department of Justice, Office of the U.S. Attorneys, Eastern District of Louisiana, *Former Phone Company Employee Sentenced to Three Months Probation for Role in Sim Swap Scam Conspiracy That Targeted At Least 19 Customers, Including New Orleans Resident*, Oct. 20, 2021, https://www.justice.gov/usao-edla/pr/former-phone-company-employee-sentenced-three-months-probation-role-sim-swap-scam; *see* Brian Krebs, *T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account*, Krebs on Security (May 2018), *available at* https://krebsonsecurity.com/2018/05/t-mobile-employee-made-unauthorized-sim-swap-to-steal-instagram-account/; Flashpoint Analyst Team, *SIM Swap Fraud Offers Account Takeover Opportunities for Cybercriminals*, Flashpoint (June 8, 2018), *available at* https://www.flashpoint-intel.com/blog/sim-swap-fraud-account-takeover/; Lorenzo Franceschi-Bicchierai, *How Criminals Recruit Telecom Employees to Help Them Hijack SIM Cards*, Motherboard (Aug. 3, 2018), *available at* https://www.vice.com/en/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-sca

good will and diligence of potentially thousands of employees and contractors scattered across thousands of stores and kiosks, most of whom will not have any meaningful experience in discerning authentic photo identification.

Third, a unified approach to customer authentication avoids subtle inconsistencies between levels of authentication that could undermine multi-factor authentication. Suppose, for example, that the Commission were to require multi-factor authentication—but only for SIM swaps and number port-outs. Suppose further that the Commission chose to permit emailed passcodes as an authentication factor. An attacker could use a stolen password to access a victim's account, change the victim's email address, and then complete multi-factor authentication for a SIM swap or port-out scam. If the Commission requires MFA for any type of account access or change, then it must additionally require MFA for any account change that could affect an authentication factor or backup authentication method.

Fourth, a unified approach will be easier to implement: carriers need only adopt one compliant customer authentication system for all account access and operations. There are a range of open-source software libraries and commercial services that enable strong customer authentication as we recommend above, with convenient integration into existing services. We foresee a minimal implementation burden even for small carriers in providing baseline secure customer authentication.

If the Commission has concerns that carriers may leverage customer authentication processes as a barrier to competition, especially in the context of number portability, we recommend addressing those concerns expressly rather than weakening authentication standards. The Commission could, for example, provide that a carrier may not implement excessively burdensome methods of authentication for port-outs that unreasonably interfere with competition.

4. **The Commission should set baseline security requirements for backup methods of account authentication.**

---

m; Lorenzo Franceschi-Bicchierai, *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring*, Motherboard (May 13, 2019), *available at* https://www.vice.com/en/article/d3n3am/att-and-verizon-employees-charged-sim-swapping-criminal-ring; Lukas I. Alpert, *UC San Diego Student Allegedly Tapped into iPhones to Steal Crypto — and Tried to Blackmail One Victim with Naked Photos*, Marketwatch (Sept. 16, 2021), *available at* https://www.marketwatch.com/story/university-of-california-student-allegedly-tapped-into-peoples-cell-phones-to-steal-their-cryptocurrency-11631580167.

If a customer forgets or loses their authentication credentials, they should have recourse to a backup method of authentication that restores access to their account. Backup authentication methods can also create security risks, however, because they can enable circumventing strong primary authentication methods.

We support the Commission's proposal to prohibit carriers from using readily available biographical information, account information, recent payment information, or call detail information as backup authentication methods.[20] As we discuss in our study, these authentication methods have significant security shortcomings. We recommend that the Commission complement these specific instances of insecure backup authentication methods with a general standard: a backup method of authentication should be reasonably designed to establish high confidence in customer identity, and it should not rely exclusively on factors that are readily available, guessable, or forgeable.

We also recommend that the Commission prohibit backup authentication based on an in-person customer service representative's assertion that they validated the customer's photo identification. As we previously discussed, this approach risks delegating too much authentication discretion to too many employees. If a carrier chooses to allow backup authentication with in-store photo identification, it should require that the customer service representative submit a scan or photo of the identification card for review using methods reasonably designed to authenticate the identification card. There are commercial services available that provide this functionality, such that it is well within reach for carriers of all sizes.

We also recommend that the Commission require customer notice (by telephone and email at minimum) and a meaningful opportunity for customer objection when processing a backup authentication request. Backup customer authentication should be a rare occurrence and inherently risks using less secure authentication methods. We believe the modest additional inconvenience of a delay is far outweighed by the security risk of immediately processing backup authentication requests.

5. **The Commission should require that carriers maintain a clearly disclosed process for customers to report account compromise, and that carriers promptly investigate reports of account compromise.**

[20] We recommend the Commission clarify that carriers may use these authentication methods in addition to other methods. The restriction should be against using these methods, individually or in combination, as the exclusive means of authentication.

There are countless anecdotes of SIM swap and port-out victims who struggle to regain control of their telephone number. In fact, during the course of our research, one of us was a victim of SIM swap fraud—and was unable to obtain prompt recourse through his carrier's customer service, so he used the same security vulnerabilities we identified to authenticate himself and return service to his phone.

We recommend that the Commission require carriers to have a clearly disclosed process for customers to quickly and easily report account compromise. If a carrier receives a credible report of compromise, it should expeditiously investigate without unreasonable delay and, if the report is accurate, restore access to the customer's account. We do not take a position on what the nature of that investigation should be or how quickly the carrier should complete it, since the details will vary by account compromise.

6. **The Commission should require carriers to track SIM swap and port-out fraud complaints.**

Carriers should be required to track SIM swap and port-out fraud complaints and report that information to the Commission. We support the Commission's proposal to require that carriers collect this type of aggregate data to measure the effectiveness of their customer authentication and account protection measures. For example, carriers could periodically report the total number of SIM swap and port-out requests, the number of successful and failed requests, the number of successful fraudulent requests, and the average time to remediate a fraudulent SIM swap or port-out. We encourage the Commission to also consider collecting a limited amount of historical data on SIM swaps and port-outs, to understand how trends in customer use and fraudulent activity are affected by changes in authentication requirements.

7. **The Commission should consider requiring that carriers provide a free software interface for determining whether a phone number was recently SIM swapped or ported.**

Insecurities in telecommunications customer authentication have negative externalities. When a carrier fails to implement strong customer authentication, it places the customer's accounts with *other* services at risk. SIM swaps are an increasing attack vector for online account compromises, especially in the financial services sector.

We recommend that the Commission consider requiring that carriers provide a free software interface (API) so that online services can instantly check whether a phone number was recently SIM swapped or ported. The API need not provide any other

information about the number, and could be integrated into the existing Number Portability Administration Center. Carriers in other countries have already implemented this approach and successfully mitigated SIM swap fraud.[21]

8. **The Commission's customer authentication rules should apply to both prepaid and postpaid services.**

We recommend that any new rules apply to both prepaid and postpaid wireless carriers. Although our study focused primarily on authentication for SIM swap requests on prepaid carriers, we anecdotally tested one account each at postpaid carriers and found—very tentatively—that some carriers may have implemented stronger authentication for postpaid accounts than for prepaid accounts. These practices almost certainly have disparate impact on low-income and minority customers. While prepaid customers may switch SIM cards more often than postpaid customers, we are not aware of evidence that SIM swapping is a frequent occurrence for typical prepaid customers.[22] And even if prepaid customers did frequently SIM swap, we would still be of the view that the security benefits of strong authentication for SIM swaps far outweigh the modest inconvenience.

* * *

We appreciate the opportunity to provide these comments and are available to answer any questions the Commission may have.

Respectfully submitted,

Benjamin Kaiser
Graduate Student, Department of Computer Science, Princeton University

---

[21] *See* Andy Greenberg, *The SIM Swap Fix That the US Isn't Using*, WIRED (Apr. 26, 2019), *available at* https://www.wired.com/story/sim-swap-fix-carriers-banks/.

[22] As a point of reference, public carrier data shows that churn is higher for prepaid customers than postpaid customers, but still very low—less than 3% of customers in the most recent quarter at major wireless carriers. Churn represents an upper limit on number porting and may serve as a rough proxy for SIM swaps. *See* AT&T, *AT&T Reports Third-Quarter Results* (Oc. 21, 2021), *available at* https://about.att.com/story/2021/q3_earnings.html; T-Mobile, *T-Mobile Delivers Industry-Leading Growth in Postpaid Service Revenues, Postpaid Customers and Cash Flow in Q3* (Nov. 2, 2021), *available at* https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2021/T-Mobile-Delivers-Industry-Leading-Growth-in-Postpaid-Service-Revenues-Postpaid-Customers-and-Cash-Flow-in-Q3/default.aspx; Verizon, *Verizon Reports Strong 3Q Revenue Growth Momentum* (Oct. 20, 2021), *available at* https://www.verizon.com/about/sites/default/files/FINAL-3Q21-earnings-release.pdf.

Mihir Kshirsagar
Technology Policy Clinic Lead, Center for Information Technology Policy, Princeton University

Kevin Lee*
Graduate Student, Department of Computer Science, Princeton University

Arvind Narayanan
Associate Professor of Computer Science, Princeton University

Jonathan Mayer*
Assistant Professor of Computer Science and Public Affairs, Princeton University
Former Chief Technologist, Federal Communications Commission Enforcement Bureau

* denotes principal comment authors.

Contact:

Website: https://citp.princeton.edu
Phone: (609) 258-5306
Email: mihir@princeton.edu