Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS ON THE NOTICE OF PROPOSED RULEMAKING

by

National Consumer Law Center on behalf of its low-income clients
and
Electronic Privacy Information Center

Submitted November 15, 2021

Margot Saunders
Senior Counsel
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Summary

In these comments, the **National Consumer Law Center (NCLC),** on behalf of its low-income clients, and the **Electronic Privacy Information Center (EPIC)** strongly support the Commission's initiatives to develop more comprehensive consumer protections from the dangers of SIM swapping and port-out fraud.

Given the significant and costly losses that are already imposed on the consumers who are victims of these fraud, we urge the Commission to require that carriers take full responsibility for protecting the identity of their customers. Specifically, the Commission should:

1) Provide strong financial incentives to providers to stop SIM swapping and port-out fraud, by making providers who fail to protect their customers private information responsible for the losses suffered by those customers.

2) Require carriers to offer a redress program that a) is fully accessible and transparent to all customers; b) provides timely responses within 24 hours after a complaint is made; c) provides full coverage of losses to customers who have been the victims of a fraudulent SIM swap or port-out fraud; and d) includes all information necessary for the customer to cooperate with law enforcement.

3) Require that in situations where multi-factor authentication cannot be reliably used to certify the identity of the person requesting the SIM swap, that the swap must occur in a retail store where identity can be appropriately checked.

4) Ensure that mobile telephone providers prohibit their employees from a) accessing CPNI until after a customer has been properly authenticated, or b) prompting leading questions or other mechanisms to enable fraudulent swaps.

5) Affirmatively require that carriers protect their customers from abuse of CPNI access by making the carriers fully responsible for any abuse committed by their employees.

6) Require carriers to include in their annual reports a detailed list of the complaints that their customers have raised regarding SIM swaps or port-out fraud, and a description of the actions they have taken to thwart further problems.

Table of Contents

Comment

I. Introduction

This comment is submitted by the **National Consumer Law Center**[1] **(NCLC)** on behalf of its low-income clients, and the **Electronic Privacy Information Center (EPIC)**,[2] in response to the Commission's initiation of a regulatory process to protect against credential theft-related harms and concomitant invasions of privacy. We appreciate the Commission's proposal to consider the best ways to prevent SIM swapping and port-out fraud pursuant to Section 222 of the Communications Act of 1934 and the Commission's CPNI Rules and LNP Rules.[3] We urge the Commission to act forcefully in this matter and require that carriers take full responsibility for protecting the identity of their customers.

[1] NCLC is a national research and advocacy organization focusing on justice in consumer financial transactions, especially for low-income and elderly consumers. Attorneys for NCLC have advocated extensively to protect consumers' interests related to robocalls before the United States Congress, the Federal Communications Commission (FCC), and the federal courts. These activities have included testifying in numerous hearings before various congressional committees regarding how to control invasive and persistent robocalls, appearing before the FCC to urge strong interpretations of the Telephone Consumer Protection Act (TCPA), filing amicus briefs before the federal courts of appeals and the U.S. Supreme Court, representing the interests of consumers regarding the TCPA, and publishing a comprehensive analysis of the laws governing robocalls in National Consumer Law Center, *Federal Deception Law*, Chapter 6 (3d ed. 2017), updated at *www.nclc.org/library*.

[2] EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC routinely files amicus briefs in TCPA cases, has participated in legislative and regulatory processes concerning the TCPA, and has a particular interest in protecting consumers from robocallers. *See, e.g.,* Br. of Amici Curiae Electronic Privacy Information Center (EPIC) and Twenty-Two Technical Experts and Legal Scholars in Support of Respondent, Facebook v. Duguid, 141 S. Ct. 1163 (2020) (No. 19-511); Br. for EPIC et al. as Amici Curiae Supporting Petitioner, Barr v. Am. Ass'n of Political Consultants, Inc., 140 S. Ct. 2335 (2020) (No. 19-631); EPIC Statement to House Energy & Commerce Committee, Legislating to Stop the Onslaught of Annoying Robocalls, April 29, 2019.

[3] *In re* Protecting Consumers from SIM Swap and Port-Out Fraud, Notice of Proposed Rulemaking, WC Docket No. 21-341 (Rel. Sept. 30, 2021), *available at* https://docs.fcc.gov/public/attachments/FCC-21-102A1.pdf [hereinafter Notice of Proposed Rulemaking].

As illustrated in the report by Princeton University entitled "An Empirical Study of Wireless Carrier Authentication for SIM Swaps" (Princeton Report),[4] American cell phone users, particularly those who rely on prepaid phones, are extremely vulnerable to having their telephone numbers hijacked by fraudsters through the process of SIM swapping and port-out fraud.[5] These are generally low-income consumers.[6] Thieves, taking advantage of the weak authentication mechanisms of the providers, have already been responsible for at least $40 million dollars of stolen funds from victims.[7] Yet, while this vulnerability has been well-known for some time, the telephone providers' continue to fail to employ adequate security systems to prevent these thefts.

These failures are shameful. And they can be easily fixed.[8] Carriers already know how to employ robust authentication procedures; they should be required to use them in all situations.[9]

---

[4] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, & Arvind Narayanan, Princeton Univ., An Empirical Study of Wireless Carrier Authentication for SIM Swaps, Proceedings of the Sixteenth Symposium on Usable Privacy and Security (Aug. 10-11, 2020), *available at* https://www.usenix.org/system/files/soups2020-lee.pdf [hereinafter Princeton Report].

[5] As noted in the Princeton Report, "Prepaid plans accounted for 21% of U.S. wireless connections in Q3 2019, or about 77 million connections. Compared to postpaid accounts, these contract-free plans are less expensive and do not require good credit, so they are more attractive to (and are often marketed to) low-income customers." Princeton Report*, supra* note 4, at 68.

[6] "Based on our experimental results for prepaid accounts, as well as our anecdotal evaluation of postpaid accounts (presented in Appendix A), we hypothesize that current customer authentication practices disproportionately place low-income Americans at risk of SIM swap attacks." Princeton Report, *supra* note 4, at 68.

[7] United States Fed. Bureau of Investigation Internet Crime Complaint Ctr., 2019 Internet Crime Report 4, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf.. Globally, SIM Swapping is on the rise. Europol, Internet Organized Crime Threat Assessment 44 (2020), *available at* file:///Users/owner/Downloads/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[8] *See* Princeton Report, *supra* note 4, at 71 ("We recommend that mobile carriers implement customer authentication for telephone support via a website or app login, or with a one-time password via a voice call. These methods do not require memorization or carrying extra devices and are easy to learn. They also should not pose significant costs to carriers because the infrastructure already exists; all carriers we examined support online accounts via websites and/or mobile applications.").

[9] *See* Princeton Report at 70-71 ("Every mobile carrier in our study, with one exception, already offers secure methods of customer authentication…Thus, carriers should begin to phase out insecure authentication methods and educate customers about these changes to reduce transition friction.").

SMS-based fraud is a major threat to consumers and is likely to become even more widespread. Credential theft through various means of tricking consumers to provide their private financial information—such as phishing, vishing, smishing, and pharming[10]—was the most prevalent cybercrime of 2020, according to the FBI's Internet Crime Complaint Center.[11] These crimes are on a steep trajectory, having grown nearly 900% over the last two years alone.[12] New tools, such as bots, make it even easier for criminals to perpetrate these digital crimes.[13]

We are encouraged by the Commission's:

- Recognition of the obstacles currently encountered by consumer fraud victims seeking remediation from their service providers after a successful attack;[14]

- Attention to consumers of pre-paid accounts, who disproportionately low-income,[15] and, who according to the Princeton Report, are likely more vulnerable to these mobile authentication attacks;[16]

- Proposal to "prohibit carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer, and to define 'SIM' for purposes of these rules as a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network;"[17] and

- Recognition of the need for all providers to prioritize improvements to their multifactor authentication processes, rather than imposing more privacy-invasive methods of verification on

---

[10] S*ee* United States Fed. Bureau of Investigation Internet Crime Complaint Ctr., 2020 Internet Crime Report 28, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf ("Phishing/Vishing/Smishing/Pharming: The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.") [hereinafter 2020 Internet Crime Report]. *See also* Federal Trade Comm'n, Scam Tag: Phishing Scams, *available at* https://www.consumer.ftc.gov/taxonomy/term/873.

[11] *See* 2020 Internet Crime Report, *supra* note 10, at 19.

[12] *Id.* at 21 (growing from 26,379 victim complaints in 2018 to 241,342 in 2020).

[13] Multiple one-time password (OTP) token interception bots now operate through Telegram. *See* Krebson Security, *The Rise of One-Time Password Interception Bots* (Sept. 29, 2021), *available at* https://krebsonsecurity.com/2021/09/the-rise-of-one-time-password-interception-bots/.

[14] *See* Notice of Proposed Rulemaking, *supra* note 3, at ¶¶ 8, 38, 41, 61, 68-73.

[15] *See id.* at ¶ 45.

[16] *See* Princeton Report, *supra* note 4, at 68.

[17] Notice of Proposed Rulemaking, *supra* note 3, at ¶ 23.

consumers, such as biometrics,[18] and its commitment to implement the new rules in an expedited manner.[19]

As the Commission has noted, most carriers know how to avoid these problems.[20] They just need to be incentivized to employ these avoidance procedures in all cases, to protect their vulnerable customers from frauds and significant financial losses.

II. The Commission should require providers to be fully responsible for consumers' losses from fraudulent SIM transfers and port-out frauds.

The single most effective protection the Commission can mandate is to establish strong financial incentives to providers for stopping the fraudulent actions. This can be done by making the providers fully responsible for the financial losses of the victims of these frauds. Indeed, the overarching point of these comments is to urge the Commission to recognize that no specific set of rules imposed on providers will be sufficient to eliminate these frauds.

Given the constantly evolving methods of fraudsters, any set of specific procedures adopted today is likely to be insufficient tomorrow. However, if providers know they will be responsible for losses caused by their system failures, they will have the incentive to respond to new security threats in appropriate ways. Indeed, as we know from the development of robust consumer protections in the credit card fraud world,[21] if providers are subject to the losses from fraud, they will develop the best defenses to fraud. This approach has the benefit of protecting both the providers and the consumers who would otherwise suffer significant losses from the frauds.

---

[18] *See id.* at ¶¶ 26, 54.

[19] *See id.* at ¶ 29.

[20] *See id.* at ¶¶ 25, 55.

[21] *See* Maya Dollarhide, Investopedia, *Who is Liable for Credit Card Fraud?* (updated July 12, 2021), *available at* https://www.investopedia.com/ask/answers/09/stolen-credit-card.asp. *See also* Federal Trade Comm'n, Lost or Stolen Credit, ATM, and Debit Cards, *available at* https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

It appears that the Commission has adequate authority to hold commercial mobile services providers responsible for fraud-related consumer losses under Section 222 of the Communications Act, through the common carrier's duty to protect consumer privacy.[22] The Act does not explicitly authorize the Commission to hold carriers responsible for customer losses as we suggest. However, in similar situations, the FCC has imposed forfeitures for violations of Section 222, where the harm to consumers from a carrier's unauthorized disclosure of CPNI was egregious.[23] In instances of SIM swapping and port-out fraud, the provider actively handing over a customer's account to a fraudster is more egregious than disclosing a portion of that consumer's account information. So, the Commission should be authorized to make carriers cover losses resulting from this egregious behavior.

III. Providers should be required to offer comprehensive remediation programs.

As the Commission recognizes, many consumers who have been the victims of SIM swaps or port-out fraud have had difficulties obtaining assistance from the carriers.[24] To remedy this problem, the Commission asks about the appropriate remediation programs that carriers should be required to create. As suggested, a dedicated and well-publicized hotline[25] should be one component.

---

[22] 47 U.S.C. 222; 2007 CPNI Order, 22 FCC Rcd at 6928 n.1 (discussing impersonating a customer to gain access to that customer's CPNI via pretexting); *see also In Re* Verizon Communications, Notice of Apparent Liability for Forfeiture and Admonishment, File No.: EB-TCD-18-00027698 (Feb. 28, 2020), at ¶ 8, (establishing inference that carrier's customer authentication practices were unreasonable where CPNI disclosed without customer authorization, absent evidence from provider demonstrating that practices were reasonable), at ¶ 59 (treating unauthorized disclosure of CPNI as "prima facia evidence that a carrier has failed to protect the information") *available at* https://docs.fcc.gov/public/attachments/FCC-20-25A1_Rcd.pdf. [Verizon Order]

[23] Verizon Order at ¶ 85-86 (finding unauthorized disclosures of consumer location information to be an egregious violation of the carrier's obligations to protect consumer privacy).

[24] *See* Notice of Proposed Rulemaking, *supra* note 3, at ¶ 38.

[25] *See* Notice of Proposed Rulemaking, *supra* note 48 at ¶ 69.

Additionally, the employees who run the hotline should be trained to provide responsive assistance in a timely manner. Calls to the hotline should trigger the following:

- Immediate assistance to the customer both to stop further losses, and to provide a safe alternative mobile telephone;

- Assurances to the customer that losses resulting from the fraud will be compensated by the provider, so long as the customer reasonably cooperates with the provider's requests for information;

- Full payment to the customer of losses that resulted from the fraud within a reasonable time period;

- An internal investigation by the customer's provider to determine how the fraud was effectuated, and if the problem was caused by another provider (or a reseller), the customer's provider should seek reimbursement for the losses from that provider;

- Direct referral by the provider to federal and state law enforcement of the fraud, along with detailed records of the fraud, unless the customer chooses not to involve law enforcement;

- An offer to the customer to notify financial institutions and creditors, the three national credit reporting agencies, and others of the fraud, to help the customer recover control over their identity, if appropriate;

- A detailed explanation of the fraud, along with an analysis of what measures the provider has taken to prevent a repeat of this breach; and

- A report of the provider's compilation of each of these steps, as applicable, in the provider's annual report to the Commission.

Finally, the Commission should require that any arbitration clauses in the providers' agreements with consumers explicitly exclude resolutions of these issues. Otherwise, consumers who have not been made whole, or who have difficulties obtaining relief for frauds that are perpetrated on them because of the provider's insufficiently strict authentication protocols, will have no meaningful way of enforcing the protections mandated by the Commission. Arbitration clauses prevent individuals from seeking relief in the courts, instead requiring consumers to engage in secret, often expensive, and often unfair tribunals that do not comply with the rules of evidence or civil

procedure established in the American judicial system. Results of arbitration proceedings are non-transparent, and non-appealable.[26]

IV. The Commission should require the most stringent additional protections.

In the Request for Comments, the Commission has identified a number of additional measures on which comments are requested. Generally, we urge the Commission to require the most rigorous of those under consideration. We have comments on several:

A. In some situations, swaps should occur only in retail stores.

The use of websites or mobile apps to employ a multi-factor authentication for SIM swapping is one way to ensure identity. But the old school way, of actually looking at an ID to ensure that the person requesting the switch is the owner, is valuable and clearly better for those consumers who do not have easy access to the internet or are uncomfortable engaging in transactions like this online. As a result, providers should always require the use of retail stores for SIM swaps except in those situations where robust multifactor authentication is available virtually to participating consumers. In stores and online, an information-based systems that cannot be easily

[26] *See* Consumer Fin. Prot. Bureau, Arbitration Study, Report to Congress Pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act § 1028(a), at § 1.4.1 (Mar. 2015), *available at* http://files.consumerfinance.gov. The Consumer Financial Protection Bureau (CFPB)'s 2015 report on arbitration in consumer financial products provides some important data on the prevalence of arbitration clauses in certain industries. *See also* Elizabeth G. Thornburg, *Contracting with Tortfeasors: Mandatory Arbitration Clauses and Personal Injury Claims*, 67 Law & Contemp. Probs. 253, 271 (2004) ("[A]rbitration clauses that provide slanted processes or limited remedies undermine the efficiency goal of personal injury law. A powerful contracting party can impose inadequate arbitration systems on countless potential plaintiffs. By doing so, it can reduce the anticipated cost of its accidents significantly and thereby decrease the deterrent effect of tort law."). Arbitrators in most arbitration cases are not required to give a reasoned explanation of the result. *See* Paul D. Carrington & Paul H. Haagen, *Contract and Jurisdiction*, 1996 Sup. Ct. Rev. 331, 347–348. Arbitrators need not follow rules of evidence. *See* Davis v. Prudential Sec., 59 F.3d 1186, 1190 (11th Cir. 1995).

exploited by fraudsters may also be useful, so long as it does not include information that fraudsters can easily access.[27]

As recognized by the Commission, online authentication is not a viable option for all consumers, especially senior consumers who may not always be technologically savvy.[28] Low-income households and households of color are also likely to have limited bandwidth available to use on their mobile phones, making online authentication more difficult for them.[29]

As a result, the best practice would be to require either a) to require that all SIM swapping should only occur in person at retail stores, where store personnel should be explicitly required to check identification or perform some other independent evaluation to ensure that the person making the request is indeed the owner of the mobile phone, or b) to permit online SIM swapping only when a demonstrably safe system has been established to verify the identity of the person making the request.

B. Customer service representatives should be unable to access CPNI until after the customer has been properly authenticated.

As suggested by the Commission,[30] there should be an unequivocal requirement that the service provider conducting the swap is fully responsible for verifying identity. As indicated by the Commission, customer service representatives who provide leading questions to the person requesting the swap facilitates the fraudster's scheme and should be flatly prohibited.

---

[27] *See* Notice of Proposed Rulemaking, *supra* note 3, at ¶ 11.

[28] *See also* Cassie McGrath, *Older adults spent an average of $1,144 on technology, up from $394 in 2019 and used devices more during COVID pandemic, AARP says* (Oct. 4, 2021), *available at* https://www.masslive.com/news/2021/10/older-adults-spent-an-average-of-1144-on-technology-up-from-394-in-2019-and-used-devices-more-during-covid-pandemic-aarp-says.html.

[29] Kendall Swenson and Robin Ghertner, *People in Low-Income Households Have Less Access to Internet Services,* Office of the Assistant Secretary for Planning & Evaluation ● U.S. Department of Health & Human Services (April 2020), *available at* https://aspe.hhs.gov/sites/default/files/private/pdf/263601/Internet_Access_Among_Low_Income.pdf.

[30] *See* Notice of Proposed Rulemaking, *supra* note 3, at ¶¶ 37, 38.

Minimizing access to private data, as well as collection and retention of that data, is a privacy and security best practice, as it reduces the risk of harm resulting from a breach.[31] In terms of data access, customer service representatives should not be able to view CPNI until after that consumer's identity has been properly authenticated. In terms of data collection, authentication methods should be no more invasive of a consumer's privacy than is absolutely necessary to protect that consumer from fraud.

C. Providers must take affirmative measures to discover and protect against fraudulent activity beyond what is specifically dictated by the Commission's rules.

As the Commission recognizes,[32] nefarious provider employee involvement in SIM swap fraud is quite real.[33] It is also likely a direct result of the fact that a significant part of the compensation paid to cell phone employees is through commissions.[34] Employees need more new accounts to boost their income, so they are incentivized to process every request to switch accounts to their employer. The employees of carriers who are either intentionally or even negligently facilitating a fraudulent SIM swap are assisting in a federal crime.

---

[31] Comments of the Electronic Privacy Information Center to the Federal Trade Commission, Standards for Safeguarding Customer Information, Request for Public Comment, Docket No. 2019-04981 (Aug. 1, 2019) at 10-11, *available at* https://epic.org/wp-content/uploads/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf (noting that personal data that was never collected can never be exposed in a breach, and noting that NTIA has considered "reasonable minimization" a "critical Privacy Outcome"); see also Federal Trade Commission, Utah Company Settles FTC Allegations it Failed to Safeguard Consumer Data (Nov. 12, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/11/utah-company-settles-ftc-allegations-it-failed-safeguard-consumer (FTC finding company's failure to delete information it no longer needed to be an unreasonable data security practice).

[32] *See id.* at ¶ 42.

[33] *See* Press Release, United States Dep't of Justice, 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), *available at* https://www.justice.gov/usao-edla/pr/former-phone-company-employee-sentenced-three-months-probation-role-sim-swap-scam.

[34] *See* Helen Akers, Career Trend, *How Are Verizon Salesmen Paid?* (updated Aug. 8, 2019), *available at* https://careertrend.com/how-are-verizon-salesmen-paid-13660582.html; Rick Suttle, Chron, *How Much Does a Cell Phone Salesman Make Annually*?, *available at* https://work.chron.com/much-cell-phone-salesman-make-annually-18991.html.

Under the federal Identity Theft and Assumption Deterrence Act,[35] one who transfers or uses another's identification with the intent to commit, or to aid or abet a violation of federal law or a felony under state law commits a federal crime. "Means of identification" is defined broadly to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[36] "Means of identification" specifically includes not just traditional forms of identification, such as name, Social Security number, and date of birth, but also "unique biometric data,"[37] "unique electronic identification number,"[38] and "telecommunication identifying information or access device."[39]

The Commission should take clear and direct action to provide a better incentive to stop this enabling of the federal crime of identity theft. The Commission should affirmatively require that carriers protect their customers from abuse of CPNI access. This requirement should be enforced by making a carrier fully responsible for any abuse committed by its employees, whether the employees acted either intentionally or negligently.

Further, the Commission should enforce this obligation by requiring carriers to include in their annual reports a detailed list of the complaints that their customers have raised regarding SIM swaps or port-out fraud, and a description of the actions they have taken to thwart further problems. This requirement is consistent with Best Practice 73 of the Number Portability Industry Forum relating to protections that group urges providers to take to stop these problems.[40]

---

[35] 18 U.S.C. § 1028.

[36] 18 U.S.C. § 1028(d)(7).

[37] 18 U.S.C. § 1028(d)(7)(B).

[38] 18 U.S.C. § 1028(d)(7)(C).

[39] 18 U.S.C. § 1028(d)(7)(D).

[40] As noted by the Commission, Best Practice 73 encourages carriers to review "incident and/or police report details if provided (official document showing case number or other verification that the matter was reported or attempted to be reported to law enforcement by reporting end user is acceptable)" and "[place] priority on resolving unauthorized ports that have a heightened severity of impact, . . ." *See* Best Practice 73, NPAC,

D. Disclosures about the availability of disabling SIM changes or freezing ports will be helpful, but not determinative.

Requiring providers to offer customers "the option to disable SIM changes requested by telephone and/or online access (i.e., account freezes or locks),"[41] or "the option to place a 'port-freeze' on their accounts at no cost to the customer to help deter port-out fraud"[42] will be helpful but is not likely to protect many consumers.

These requirements would do no harm, and indeed the ability to freeze one's own account is an excellent way for an individual consumer to guard against fraud.[43] And, for a few consumers these options may provide meaningful protections. But the Commission should not assume that requiring a disclosure about the availability of these options will actually protect many consumers. Instead, these options will provide only a confusing and little-used voluntary mechanism that will not accomplish much. Disclosures and the ability to freeze one's account are valuable only to those consumers who are savvy enough to a) understand the dynamics involved in freezing, b) understand that the benefits of freezing outweigh the extra burdens imposed (such as requiring that the consumer go through a series of steps to unfreeze the account, and c) actually follow through and freeze one's account. An illustration of this dynamic is that only ten percent of all consumers freeze their credit files even with the well-publicized—and escalating—threat of data breaches and identity theft.[44]

Number Portability Best Practices, *available at* https://numberportability.com/industryinfo/lnpa-working-group/lnp-best-practices/?page=1

[41] Notice of Proposed Rulemaking, *supra* note 3, at ¶ 39.

[42] *Id.* at ¶ 57.

[43] *See* Federal Trade Comm'n, What To Know About Credit Freezes and Fraud Alerts, *available at* https://www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts.

[44] *See* Herb Weisbaum, NBC News, *Worried about data breaches? Now you can freeze your credit for free* (Sept. 21, 2018), *available at* https://www.nbcnews.com/better/business/worried-about-data-breaches-now-you-can-freeze-your-credit-ncna911101.

As the Princeton Report notes, and the Commission acknowledges, the consumers most susceptible to fraudulent SIM swaps are low-income, and therefore much more likely to be less sophisticated about these processes and less likely to understand the benefits of using these options.

V. Conclusion

We support the Commission's attention to this problem, and its consideration of various ways to avoid its continuation in the future. We urge the Commission to consider our proposals to clearly place the burden of losses that result from fraudulent SIM swaps on the provider who processed the fraudulent swap, and to limit collection of and access to sensitive consumer information beyond what is strictly necessary for verification. The threat of covering those losses for harmed consumers should provide meaningful incentives to the providers to ensure that the frauds are stopped.

Respectfully submitted, this the 15th day of November 2021, by:

Margot Saunders
Senior Counsel
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036
msaunders@nclc.org

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org