FIDO Alliance Input to the FCC

NPRM on Rules to Prevent SIM Swapping and Port-Out Fraud

November 2021

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to provide comments to the Federal Communications Commission (FCC) on its Notice of Proposed Rulemaking (NPRM) on Rules to Prevent SIM Swapping and Port-Out Fraud.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO2 standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy MFA tools.

As the White House's recent draft Federal Zero Trust Strategy notes, FIDO2's Web Authentication standard *"is supported today by nearly every major consumer device and an increasing number of popular cloud services."*[1] Apple, Google, and Microsoft have all embedded support for FIDO2 at the device, operating system, and browser level, enabling new models for deployment phishing-resistant MFA to be "built in" rather than "bolted on."

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

The sharp rise in SIM Swap attacks is one of many reasons that companies including major U.S. Mobile Network Operators (MNOs) have embraced FIDO authentication over the last five years. While criminals and foreign adversaries are able to use SIM Swap attacks to undermine some weaker forms of multi-factor authentication (MFA) such as one-time passcodes (OTPs) transmitted via SMS, FIDO authentication is not susceptible to these attacks.

[1] https://zerotrust.cyber.gov/federal-zero-trust-strategy/

As the FCC considers new regulations here, we offer four primary comments:

1. **SMS was never designed to be used for authentication – and the sooner organizations stop using SMS, the sooner the United States can remove the core incentive for criminals to launch SIM Swap attacks.**

   To truly eliminate SIM Swap attacks, the best way to do so is to get companies and organizations to shift from SMS-based authentication to more secure forms of MFA. This will remove most of the incentives for attackers to launch SIM Swap attacks.

   As the NPRM points out, NIST advised organizations to stop using SMS for authentication in 2016, and the attacks against SMS-based authentication have only increased since then. However, many organizations continue to rely on SMS as a second factor because it is cheap and easy to deploy.

   While the FCC may not be able to prevent the use of SMS for authentication, any role it can play in working with other parts of government (such as CISA, NIST, and financial regulators) to discourage its use and push the country toward more secure authentication methods means that the incentives to launch a SIM Swap attack will go down significantly.

2. **FCC has proposed four *Customer Authentication Requirements for SIM Change Requests* that are focused on authentication methods that rely on already-compromised authentication technologies – and may create disincentives to stronger tools such as FIDO authentication being used.**

   Each of the four methods proposed might help to temporarily slow down SIM Swap attacks, but they are all based on authentication methods that are known to be easily compromised. We expect that attackers would simply adapt their attack methods to target these new authenticators, with the net effect being no significant slowdown in the pace of SIM Swap attacks.

   Below we review each of the four proposed methods and detail the problems with them:

   - *Pre-established password:* It has been well-established in the security community that passwords offer minimal security. [2] Passwords are routinely phished and reused by consumers across sites. They are also frequently forgotten, pushing customers (or attackers who pretend to be a customer) into the account recovery process, allowing attackers to circumvent authentication controls. A password will not deter any determined attacker.
   - *OTP sent via text message:* FCC itself in paragraph 24 notes that "SMS-based text messages could be easily intercepted and re-routed…" and the NPRM cites several other examples of where SMS-based authenticators are frequently compromised. While in theory SMS OTPs could help to serve as a check on an attacker who was claiming a phone was lost or stolen – since the rightful holder of the phone would get a message to verify that they wanted to migrate their number to a new phone – attackers are routinely targeting these OTPs in other sectors with automated attacks to trick people into handing over these codes. [3]

     Additionally, any authentication method premised on an OTP being sent by SMS assumes that consumers are in possession of their phone. But if their phone is lost or stolen – two use cases that account for a significant percentage of phone number migrations – this authentication method is useless.

[2] For an excellent description of why passwords and password strength are largely irrelevant to guarding against modern attack vectors, see https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

[3] Earlier this month, Motherboard published an article detailing how these attacks are now being automated and executed by bots. https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo

- Passcode sent using a voice call: The issues with voice passcodes are the same as with OTP codes sent via SMS. Attackers routinely trick consumers into handing these codes over. And they assume possession of the phone – if a consumer's phone is lost or stolen, this method does not work.
- OTP sent via email. While there are some benefits to this sort of "out of band" approach, email accounts are routinely compromised – in large part, because most consumers have not turned on MFA to protect those accounts. Given the ease of taking over email accounts, any mandate to rely on email as an authentication channel would just push attackers to focus more on compromising those accounts – much as the frequent use of SMS for authentication has made carriers a target for SIM-Swap attacks.

In summary, while each of the four proposed authentication methodologies might create some additional friction for attackers, the FCC should not be under any illusion that any of these methods will offer enough security to meaningfully address the threat of SIM Swap attacks.

That said – all MFA is not the same, and there are other more secure methods of authentication that could stop these types of attacks on legacy authentication tools. In general, industry and government are moving away from knowledge-based approaches to authentication (i.e. passwords) to those that are possession-based, such as authentication based on the FIDO2 standards, which cannot be phished given that they use asymmetric public key cryptography in authentication.

The new Federal Zero Trust Strategy published in September explicitly recognizes the difference between "legacy" forms of MFA and more modern, phishing-resistant approaches to authentication, noting:

> *"Many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."*

The Strategy goes on to note:

> *"Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks. The Federal Government's Personal Identity Verification (PIV) standard is one such approach, and so will help many agency systems meet this baseline. The World Wide Web Consortium (W3C)'s open "Web Authentication" standard, another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services."*

Notably, two major U.S. mobile network operators (MNOs) already support FIDO authentication for their customers, meaning that it is widely used in customer-facing accounts today. We believe that for use cases where a consumer is still in possession of their phone, relying on FIDO authentication as part of verifying possession of that phone could be effective in stopping SIM Swap attacks.

Additionally, customers who have FIDO Security Keys could use those keys in the event a phone was lost or stolen as one way to prove ownership of that phone and its corresponding account. Security keys are hardware cryptographic devices that are not bound to a specific device such as a phone, but instead can be used to authenticate across multiple devices. We note that the White House Federal Zero Trust Strategy calls on government agencies to make increased use of security keys in citizen-facing applications, noting:

> *"Public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication. Because most of the general public will not have a PIV or CAC card, agencies will have to meet this requirement by providing support for Web Authentication-based approaches, such as security keys."*

Given FIDO's widespread adoption today among MNOs – as well as support for use of FIDO standards from the White House, NIST,[4] the FFIEC,[5] the FTC,[6] and other regulators, we are a bit perplexed as to why FCC's proposal was limited to four legacy authentication methodologies that are all easily compromised.

To that point, we have some concerns that if the four authentication methodologies are the only ones listed in the regulation, that it may discourage the use of stronger, more innovative approaches to authentication. One constant in cybersecurity is that threats are constantly evolving, as are the tools used to stop threats. But regulations are permanent, or in a best-case scenario, infrequently updated. Any regulatory approach that seeks to tie MNOs to using specific authentication technologies is certain to fail to keep up as threat and security both evolve.

3. **Beyond the U.S., other governments such as Australia and the United Kingdom (U.K.) have not only referenced FIDO standards in their guidance but FIDO certification as well. In 2020, both the Australian and U.K. governments specifically called out FIDO standards and certification programs by name in their MFA guidance.**

- The Australian Cyber Security Centre (ACSC) – via its "Essential Eight" guidance on "Implementing Multi-Factor Authentication" – specifically recommends that implementers only use security keys have been certified by the FIDO Alliance.[7]

- The U.K. – as part of its "Using authenticators to protect an online service" guidance (Good Practice Guide 44) published jointly by the Government Digital Service and Cabinet Office– notes that an authenticator token "is high quality if it has been independently tested to prove it meets industry standards, such as the Common Criteria guidelines, FIDO or NIST FIPS 140-2."[8]

FIDO Alliance's certification program has gained this recognition thanks to the robustness and rigor of its program. Moe than 850 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.[9] Indeed some governments have also pursued their own FIDO certifications – for example, Germany's Federal Office for Information Security (BSI).[10]

We believe it will be helpful for MNOs looking to implement FIDO authentication to know that they should look for those authentication solutions that have been certified by FIDO Alliance, in line with similar UK and Australia guidance. FCC should consider pointing to FIDO certification in any regulations for authentication that it puts forward.

4. **It will be important for the FCC to consider other "identity lifecycle" issues such as identity proofing and account recovery; a new FIDO certification program can help here.**

More secure means of authentication will help to stem the tide of SIM Swap attacks for use cases when someone has their phone in their possession. Most SIM Swap attacks (and many legitimate customer requests),

[4] https://www.nist.gov/system/files/documents/2020/07/02/SP-800-63-3-Implementation-Resources_07012020.pdf

[5] https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf

[6] https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial

[7] See page 5 of https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Implementing%20Multi-Factor%20Authentication%20%28June%202020%29.pdf. Note that this guidance currently references FIDO U2F certification, calling for implementers to *"use U2F security keys that have been certified to the latest U2F specification version."* It is expected that the next revision will shift the focus to FIDO2.

[8] https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services

[9] See https://fidoalliance.org/certification/ for more details on FIDO's certification programs

[10] See https://fidoalliance.org/authenticator-certification-hits-a-new-milestone-with-first-l3/

however, are centered around use cases where a phone is claimed to be lost or stolen – meaning that most possession-based factors will not be useful in many of those cases.

Reports of lost or stolen phones instead trigger an account recovery process largely reliant on carriers having an easy means to determine that a customer is who they claim to be. This is an area where identity proofing and account recovery solutions are lacking.

One of the more promising approaches to remote identity proofing has been the emergence of products that ask consumers to help validate their identity through two simple steps: 1) taking a snapshot of their ID with their phone – that is then authenticated by software that can differentiate legitimate credentials from counterfeits – and then 2) take a selfie that is then matched against the photo on the ID.

Dozens of products embracing this core model are now in the market, though their performance varies wildly. To bring a standardized approach to testing these products, FIDO Alliance has launched a new Identity Verification and Binding Working Group charged with creating performance standards for remote ID verification products that can then be used by independent labs to test different products' performance. This testing and certification program should launch in the next year, and may be another useful tool that the FCC can guide MNOs toward as a way to protect consumers.

We greatly appreciate the FCC's consideration of our comments. We look forward to further discussion with FCC on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this response. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should FCC staff officials desire to learn more about how FIDO authentication and how its certification programs work.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.