FIDO Alliance Comments to the Chilean Financial Market Commission (CMF)

April 2026

Comments on the Draft Regulation - Modification of NCG N°538

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to provide input to the to Chilean Financial Market Commission (CMF) on its *Draft Regulation - Modification of NCG N°538 on Security Measures and Authentication of Operations (Law No. 20.009).*

As background, 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, cryptocurrency, fintech, and payments – as well as many of the security vendors those firms turn to when it comes to guarding against attacks on identity verification and authentication.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the fourteen 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 FIDO standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication – such as passkeys and security keys – that are both more secure and also easier to use than legacy authentication tools. They are supported by a broad ecosystem of more than 1000 products that have been certified as meeting the FIDO standards, ensuring that enterprises of all sizes are able to choose from a variety of interoperable, standards-based products to meet their authentication needs. Moreover, with the FIDO Web Authentication protocol being a W3C standard, ever major browser and platform ships with native support for FIDO, making phishing resistant authentication as easy (or often easier) to deploy as legacy authentication tools.

FIDO Alliance welcomes and values the Commission's continuous effort to strengthen the cybersecurity of the Chilean financial ecosystem under Law No. 20.009.

We deeply understand and support the CMF's concern for ensuring financial inclusion. It is imperative to ensure that segments of the population with lower levels of digitalization – particularly older adults – are not excluded from financial services due to operational difficulties when adopting new Strong Customer Authentication (SCA) mechanisms.

To that point, we do not have any objection to preserving the use of legacy MFA tools such as printed data sets for segments of the population who are not in a good position to adopt more modern SCA approaches such as passkeys. Banks need to "meet their customers where they are at" and it takes time to migrate away from other legacy tools.

That said, while we understand the reason to preserve the use of these printed cards and support the government's decision, we do want to highlight a few issues for CMF's consideration, and also suggest an amendment to the proposed language that might help to accelerate Chile's migration to more secure forms of SCA:

1) **Phishing is becoming a bigger problem – and the use of printed cards will leave users of those cards vulnerable to phishing attacks.**

   Across the globe, attackers have caught up with many of the legacy tools that are used to safeguard authentication. Adversaries have devised ways to phish legacy tools based on OTPs, printed cards with codes, or push-based authentication apps, creating an imperative across the globe to move consumers to more modern, phishing resistant tools for authentication.

   These attacks are being fueled by the rise of generative AI, which is making it easier for adversaries to craft well-designed phishing attacks that fool more users. The entire phishing process can be automated using Large Language Models (LLMs), reducing the cost of phishing attacks by more than 95% while achieving equal or greater success rates.[1]

   Many of these phishing attacks are enabled by deepfake technology. Deepfake incidents in the fintech sector increased by 700% in 2023 compared to the previous year.[2]

   Given this rapid evolution in attacks against authentication, it is thus imperative that any government regulatory action which allows for the use of legacy, phishable authentication also takes steps to incentivize the retirement of these legacy tools over the next few years.

2) **Many other governments are now calling specifically for the use of phishing-resistant authentication to protect consumers in financial services.**

   - ENISA last year published Technical Implementation Guidance for organizations seeking to comply with the NIS2 cybersecurity directive in the European Union.[3] The new guidance specifically says ""Wherever possible, use-phishing-resistant MFA" and lays out a hierarchy of MFA that reads:

     "The use of phishing-resistant MFA is recommended. Below is a list of currently available solutions

[1] See https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
[2] See https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5
[3] See https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

ordered from strongest to weakest.

- *Strong: Phishing-resistant*
  - no shared secrets, not vulnerable to attacker-in-the-middle;
  - protected cryptographic private key that can be securely registered to:
    - *a domain, in accordance with Fast Identity Online (FIDO) and W3C WebAuthn standards;*
    - *a trust provider, following public key infrastructure and International Telecommunication Union X.509 standards.*

- *'Medium' MFA, for example:*
  - *push notification, number matching or application based.*

- *'Last resort' MFA, for example:*
  - *text message or email OTP"*

- ENISA and CERT-EU also highlighted the importance of FIDO in a 2022 publication entitled "Boosting Your Organization's Cyber Resilience (JP-22-01),"[4] noting:

  "If possible, avoid using SMS and voice calls to provide one-time codes and consider deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."

- In the US, the National Institute of Standards and Technology (NIST) has advised organizations to prioritize phishing-resistant authentication, noting in its Digital Identity Guidelines (SP 800-63B)[5]:

  *"In all cases, verifiers **SHOULD** encourage the use of phishing-resistant authentication at AAL2 whenever practical since phishing is a significant threat vector."*

  In addition, NIST notes that "Look-Up Secrets" such as the printed cards used in Chile are "not phishing-resistant."

- Also the US, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory[6] echoing the concerns of ENISA, noting:

  "Not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems."

  The CISA guidance goes on to note:

  "While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort," and also notes that *"The only widely available phishing-resistant authentication is FIDO/WebAuthn authentication."* – although it notes that PKI-based MFA is also phishing-resistant, if not as widely available.

[4] See https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience
[5] See https://pages.nist.gov/800-63-4/sp800-63b.html
[6] See https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

- Also in the US, an August 11, 2022 circular[7] from the U.S. Consumer Financial Protection Bureau (CFPB) states:

> *"MFA solutions that protect against credential phishing, such as those using the (FIDO) Web Authentication standard supported by web browsers, are especially important."*

- We also note that a 2023 Cyber Safety Review Board (CSRB) report[8] of the attacks associated with the LAPSUS$ Group stated:

> *"In the past decade, the emphasis on MFA has driven the adoption of more secure solutions to improve resiliency against attacks and phishing in particular. Enterprise and consumer adoption of MFA has been a beneficial step forward away from use of just passwords for authentication. However, the Board's review found that the types of MFA used broadly in the online ecosystem today are not sufficient for most organizations or consumers defending against the type of attacks described in this report.*
>
> *"In particular, OTP delivery and push notifications using SMS and voice calls (and even email) are vulnerable to social engineering and SIM swap attacks, and the attacker ecosystem is readily capable of exploiting these weaknesses. A lucrative SIM swap criminal market is enabling pay-for-access to victim mobile phone services with a focus on hijacking SMS messages and voice calls. SMS was not designed to transact sensitive information such as OTPs, and its wide use as such incentivizes criminals to perform SIM swap attacks, porting fraud, and similar techniques.*
>
> *"Web and mobile application developers should leverage Fast IDentity Online (FIDO)2-compliant, hardware-backed solutions built into consumer devices by default. Use of these built-in tokens should have easy integration with applications and web-based services, leveraging standards such as WebAuthn and technologies such as Passkeys".*

3) FIDO Alliance is investing in user experience (UX) initiatives to make it easier for all populations to use passkeys.

Through our User Experience Working Group (UXWG), the Alliance continuously develops and refines design guidelines[9] based on comprehensive consumer research. The goal of these initiatives is to help relying parties, such as financial institutions, implement authentication flows that eliminate technological friction, transforming traditionally complex security processes into simple, everyday interactions - such as using the fingerprint or facial recognition they already use to unlock their own personal devices.

Furthermore, the FIDO Alliance equips the industry with practical tools and resources, such as implementation rubrics and specialized roll-out guides available in *Passkey Central*[10], to empower organizations to independently audit and optimize their user interfaces. These ongoing UX and enablement investments aims to ensure all populations can easily use passkeys.

Furthermore, the FIDO Alliance stands ready to collaborate with the Chilean government, the CMF, and local financial institutions to develop and support public education campaigns. By raising awareness

[7] https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/
[8] https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf
[9] See https://www.passkeycentral.org/design-guidelines/
[10] See https://www.passkeycentral.org/

about the risks of legacy authentication and the benefits of modern, phishing-resistant methods like passkeys, we can jointly help incentivize consumers to transition towards these safer technologies, ensuring a secure and inclusive digital financial ecosystem in Chile.

Proposed changes to the text (Section V)

To balance user protection with financial inclusion, and to ensure that the transitional exception does not become a structural disincentive for issuers to invest in better technology and usability (UX), we propose enriching the wording of the penultimate and ultimate paragraphs of the proposed regulation (Section V), adding the highlighted texts:

> "The inclusion of clients in the groups referred to in the previous paragraph may only be carried out after the issuer has made its best efforts to provide alternatives to these clients, **prioritizing the provision of highly usable and phishing-resistant authentication methods (such as passkeys or physical security keys)**, and will be possible exclusively regarding existing clients as of the date of issuance of this regulation, who must also be informed of the risks entailed by maintaining the authentication methods they have been using."

Additionally, we suggest modifying the reporting mandate in the last paragraph to foster continuous innovation:

> "(...) Furthermore, they must send a semi-annual update on the number of clients who have ceased to be part of these groups, who may not be included in them again, **including a report on the new phishing-resistant authentication technologies evaluated or implemented to progressively reduce the exempted population**."

We appreciate CMF's considerations of our comments and suggestions. Should you have any questions on our submission – or would like to learn more about FIDO standards and certification programs – please reach out to our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, our Head of LATAM, Diego Zavala, at diego@fidoalliance.org, or our policy advisor, Jeremy Grant, at jagrant@venable.com.