April 25, 2025

Mr. Eric Ducoulombier
Head of Unit – Retail Financial Services
DG-FISMA
Rue de Spa 2
1000 Brussels, Belgium

Dear Mr. Ducoulombier,

We greatly appreciate the willingness of your colleagues to meet last month with the FIDO Alliance and our members to discuss issues around Strong Customer Authentication (SCA) – and the ongoing effort to update the Second Payment Services Directive (PSD2) and create a new Payment Services Regulation (PSR).

As follow-up to our recent discussion, we wanted to suggest some minor edits to the draft PSR that we believe would help to ensure that the Regulatory Technical Standard (RTS) for SCA can continue to serve as an effective guard against adversaries who seek to compromise weak authentication technologies to steal money and defraud European consumers and businesses.

As we have noted in our previous discussions: while SCA has helped to reduce theft and fraud tied to weak authentication, the threat landscape has changed significantly since the RTS was finalized in 2017. Legacy technologies used in SCA – such as one-time passcodes (OTPs) delivered through SMS and apps, as well as authentication tools tied to push notifications – have become much more vulnerable to phishing attacks. And while these attacks existed in 2017, adversaries have become much more adept at finding new ways to compromise these legacy authentication tools at scale.

Over the last 24 months, our members – many of whom are financial services firms – report seeing a sharp increase in the number of automated phishing attacks, many of which are being enabled by the widespread availability of attack tools powered by generative artificial intelligence (Gen AI). These new attack methods have taken what once required a resource-intensive and time-consuming effort to compromise authentication codes and turned them into an attack that is cheap to launch and can be executed at scale. It is clear that the tools used in SCA will need to evolve if they are to continue to protect European consumers and businesses.

Against this backdrop, we have seen governments in Europe and across the globe point to the importance of "phishing-resistant authentication" that can automatically block and defeat these phishing attacks.[1] With this, FIDO Alliance and its members have brought the new technology of "passkeys" to the market – phishing-resistant credentials that can securely and easily log consumers in to online services without a password. The European Commission (EC) has adopted passkeys to enable passwordless multi-factor

[1] See https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html and https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools/Factsheet_Mature_authentication+EN.pdf,

authentication into its EU Login service,[2] and a number of governments across the globe have recognized passkeys as a logical way for consumers to have a more secure and convenient way to authenticate across a range of use cases.[3] The fact that passkeys are delivered via the W3C's Web Authentication (WebAuthn) standard[4] – and that every major browser and platform ships with native support for that standard – has helped to drive the rapid adoption and government recognition of passkeys. In payments, we have seen passkeys be used both on their own, and in some high-value use cases, also combined with other security tools to provide additional layers of protection.[5]

As we noted in our recent discussion, however, we continue to get questions as to whether passkeys fully comply with the requirements of the 2017 RTS. This is inhibiting adoption of passkeys in the European financial services market, even as the technology takes off across the globe and in other sectors in Europe. For this reason, the new PSR and the presumed update of the RTS on SCA that would follow presents a timely opportunity to update some aspects of the current SCA policies to ensure that solutions leveraging passkeys and other innovations in authentication are more clearly permitted.

While we expect the bulk of the updates will need to be addressed in the revised RTS, there are a handful of minor changes to the draft PSR that would help to ensure that a revised RTS can accommodate passkey-based solutions and other innovations in authentication, as well as be flexible enough to address future threats to authentication (or innovations to guard against those threats) in the years to come. Below we detail our suggestions:

Proposed Change	Rationale
Article 89, Section 2 (b) **Amend to read**: the need to ensure the safety of payment service user's funds and personal data, ***including guarding against phishing attacks;***	As noted above, many legacy authentication solutions are now easily phished, and new automated tools are making it easier than ever for attackers to successfully phish SCA. This language would ensure that the SCA RTS evolves to address these risks. Additionally, because the EU Digital Identity Wallet initiative has already embraced the use of passkeys and the Web Authentication standard in its implementing regulations and Architecture Reference Framework,[6] adding this

[2] See https://trusted-digital-identity.europa.eu/eu-login-help/can-i-use-passkey-eu-login_en

[3] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_Passkeys.html , https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications, and https://www.ncsc.gov.uk/blog-post/passkeys-promise-simpler-alternative-passwords

[4] FIDO Alliance partnered with the W3C to develop the Web Authentication standard

[5] See, e.g., https://corporate.visa.com/en/products/visa-payment-passkey.html

[6] See Annex V of https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402979 and https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v1.7.0/docs/architecture-and-reference-framework-main.md#47-pseudonyms

	language would help to ensure that the EUDI wallets can be used to support SCA requirements.
Complement the change above by slightly amending Recital 107 to read: Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. In the area of fraud, the major innovation of Directive (EU) 2015/2366 was the introduction of Strong Customer Authentication (SCA). The Commission's evaluation of the implementation of Directive (EU) 2015/2366 concluded that strong customer authentication has already been highly successful in reducing fraud. ***However, as the fraud landscape evolves and new threat vectors such as credential phishing become more prevalent, it is imperative that SCA evolves to address these threats and enable new innovations in authentication.***	See above.
Support EU Parliament's suggested Recital 107a – with a minor change: In order for consumers to benefit from continued strong SCA, and for SCA to remain an effective tool in the fight against fraud in electronic payments, it is appropriate that the application of SCA be risk-based ***and outcomes-based***. In turn, the rules on SCA should provide sufficient flexibility for innovation within the payments sector, including in the development of new SCA solutions ***in order to enable both secure and convenient payment experiences.***	We believe that some of the current questions around the 2017 RTS are tied to how prescriptive the current RTS requirements are. An approach that allows more room for risk-based and outcomes-based solutions would make it easier for new innovations like passkeys to be adopted, without requiring another re-write of the RTS. If a PSP can demonstrate that the use of passkeys (or other new innovative security tools) leads to lower fraud rates than legacy SCA solutions, we believe they should be permitted.

Support EU Parliament's suggested change to Article 89, which reads: The EBA, before submitting its draft regulatory technical standards to the Commission, shall hold an open consultation with public and private stakeholders in order to ensure that the most up to date advances in technology and payment processing, as well as the specificities of business to business and business to government transactions, are taken into account in the draft regulatory technical standards.	We believe EBA's process to update the RTS would greatly benefit from an open consultation. This would allow them to gain a more comprehensive understanding about the ways that the threat landscape has evolved since 2017 – and how it might continue to evolve as new AI-powered attack tools become more common – as well as new technologies that can defend against these threats.

Beyond these core points above, we have two additional suggestions:

- **Article 85, Section 12**
  We agree that the definition of whether authentication is "strong" should not be dependent on whether each authentication element belongs to a different category. Indeed, our take is that the idea of requiring two factors is outdated as a way to measure the strength of an authentication solution; we believe that a single factor that is phishing-resistant and resistant to other vulnerabilities can be stronger than two factors that are both phishable or otherwise easily exploitable. However, we believe that a solution that relies solely on two knowledge factors should not be considered "strong," given how easy it is to compromise knowledge factors.

  For this same reason, we believe that the continued use of SMS as an authentication element should be restricted. Indeed, the myriad vulnerabilities of SMS as an authentication tool have led the EC to announce plans to phase out SMS authentication for its EU Login service by mid-2025. If the EC deems SMS to be unsuitable for EU Login, we believe it should also be deemed unsuitable for SCA.

- **Article 87**
  We believe the requirement for a PSP to enter into a formal outsourcing agreement for SCA with a security provider might create material barriers to the use of passkeys, given that consumers might choose to rely on a variety of "passkey providers" to store their credentials. For a PSP to allow consumers to have choice in passkey providers, a requirement for a PSP to enter into an agreement with each passkey provider will serve as a barrier to promoting competition and innovation.
    - If an issuer must enter into a bilateral outsourcing agreement for each authentication solution (including the ability to access a passkey from various passkey providers), they will likely only do so for solutions that are already at scale and for a limited number of solutions, leaving smaller players that may have a lower coverage of the overall transactions out of the picture.
    - On the third-party side, smaller companies may not have the resources required to comply

with these agreements.

- Regulation should differentiate between various authentication methods (depending on the role/level of control that issuers have in the process) and clarify that when issuers remain in control of the SCA process, outsourcing agreements are not needed.
- To the extent credentials stored in a country's EUDI wallet would be used for SCA, these requirements would also have a very negative impact on the ability of PSPs to leverage those wallet-based solutions.

We greatly appreciate DG-FISMA's consideration of our comments. We look forward to further discussion with you 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 letter.

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