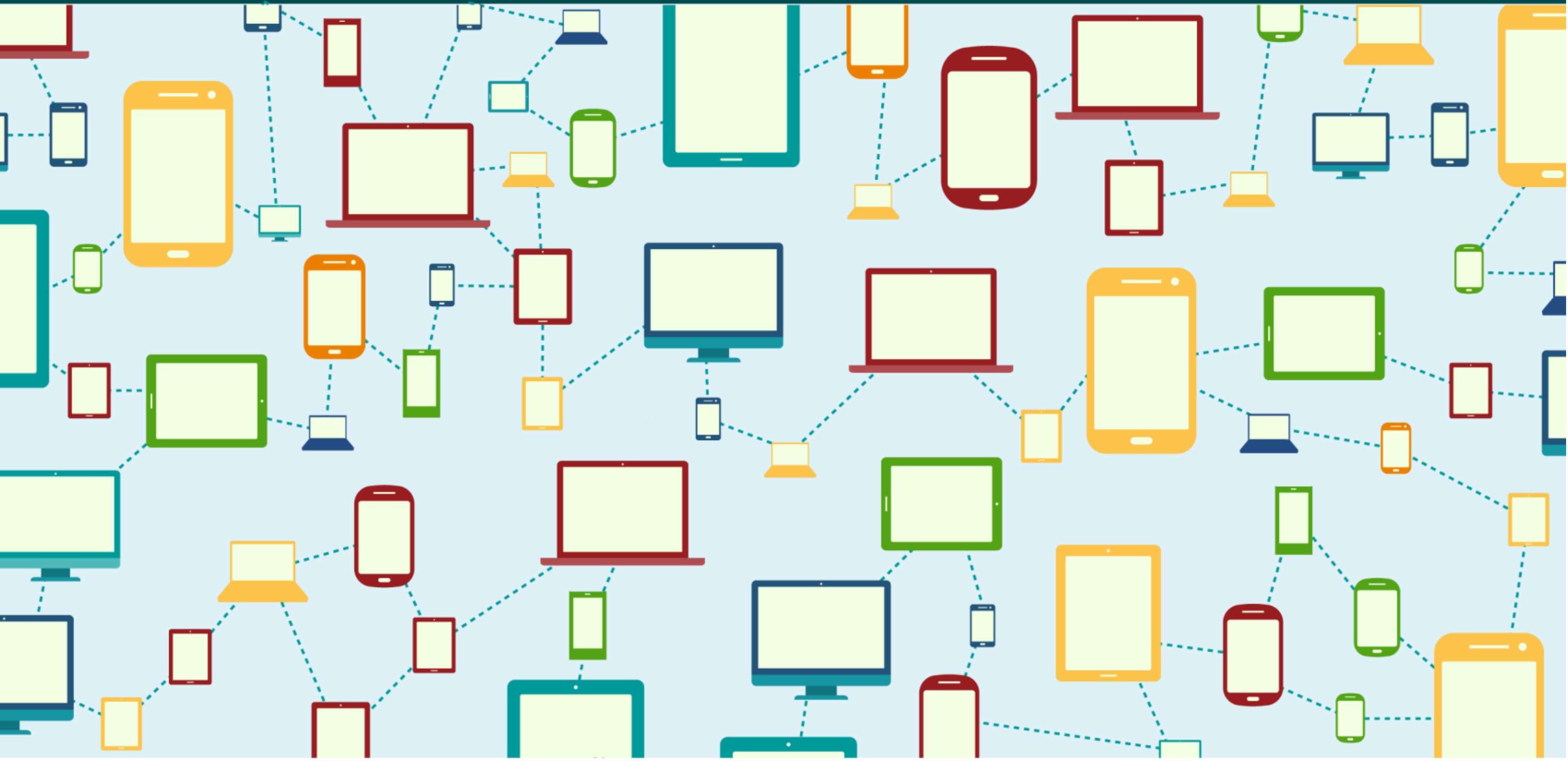

# FIDO Alliance Response to the European Banking Authority (EBA)

# Consultation on the Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)

## August 2018

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the Consultation on the Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) published by the European Banking Authority.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to creation of standards for Multi-Factor Authentication (MFA).

We provide a unique perspective to this discussion given that our members include both banks and FinTech firms, as well as major payment card networks, mobile network operators, hardware manufacturers, software vendors and government agencies. Collectively, the FIDO Alliance represents the largest consortium in the world focused on authentication – one whose members have deep expertise in designing and deploying major systems at scale that allow innovation to flourish while also protecting security and privacy.

Our 35 board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership.

Given the focus of the FIDO Alliance on authentication, our comments here are largely focused on the portions of the draft that impact the way in which Strong Customer Authentication (SCA) will be implemented.

**Question 1: Do you agree with the EBA's assessments on KPIs and the calculation of uptime and downtime and the ASPSP submission of a plan to publishing statistics, the options that EBA considered and progressed or discarded, and the requirements proposed in Guideline 2 and 3? If not, please provide detail on other KPIs or calculation methods that you consider more suitable and your reasoning for doing so.**

We believe the EBA has taken a reasonable approach here.

**Question 2: Do you agree with the EBA's assessments on stress testing and the options it considered and progressed or discarded, and the requirements proposed in Guideline 4? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

**Question 3: Do you agree with the EBA's assessments on monitoring? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

**Question 4: Do you agree with the EBA's assessments on obstacles, the options it considered and progressed or discarded, and the requirements proposed in Guideline 5? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

In particular, we believe EBA has taken a particularly thoughtful approach on this topic in three areas:

1. The finding, in item 35, that *"what is commonly referred to as 'redirection' is not in itself an obstacle."*

2. The finding, in item 40, that: *"any method of access may be an obstacle depending on how it has been implemented and CAs should consider the user experience, whether the access method accommodates all methods of authentication and how this impacts on the user experience or if it creates delays and friction in the customer journey when assessing an exemption application for a dedicated interface that provides for access using only a single method of access."*

3. The finding, in item 36, that "here is not *"a requirement in PSD2 or the RTS for an ASPSP to provide more than one method of access"* when it comes to supporting different access models.

A number of our members have been concerned that language in the RTS might preclude the use of redirect implementations that are both highly secure and highly convenient for consumers – and instead push ASPSPs and TPPs to less secure and less convenient models of authentication. While there are some ways to implement a redirect model that might inhibit a good customer experience, there are other ways to leverage redirect to deliver a best-in-class solution for the customer.

One of the most notable innovations driven by the FIDO Alliance and its members has been the advent of single-gesture, passwordless multi-factor login experiences that are both more secure and more convenient than older, legacy approaches to multi-factor authentication.

To this point, we offer a comparison of two different login experiences: one via a redirect model using FIDO authentication and a second via an embedded model using passwords and OTP.

- The first experience is based on a redirect model where a PSP briefly redirects the PSU to an ASPSP's login page, which then prompts the PSU to login via FIDO. Because FIDO supports "single gesture" authentication, the only step the PSU needs to take to authenticate is to place her finger on a sensor or take a selfie; that biometric is then matched locally on the PSU's device, which then unlocks the second factor: a private key that is used to sign a cryptographic challenge presented by the ASPSP. Once authenticated, the PSU is then routed back to the PSP's interface.

  The entire process takes less than two seconds, and the only thing the PSU is asked to do is present a biometric. The signing of the cryptographic challenge takes place entirely behind the scenes, without anything being demanded of the PSU.

- The second experience is based on an embedded model that requires a PSU to take multiple steps to authenticate:
  1. First, the PSU must enter a username and password into the PSP's application
  2. Then the PSU is prompted to enter the second factor: an OTP. To do so, she must launch a separate OTP app or retrieve an OTP code sent by SMS, then view and remember the 6-digit code
  3. Then, she must switch back to the PSP app and key in the 6-digit code without error, or without that code expiring.

  The entire process may take upwards of 15 seconds, and requires the PSU to take multiple steps to authenticate.

The redirect model in this case delivers a customer journey and user experience with less obstacles, delays and friction. Moreover, use of the redirect model is far more secure here, given that OTP codes are often phished just like passwords, as has been documented by NIST and other security experts. FIDO authentication – given its use of public key cryptography – is resistant to phishing attacks and other tools used to compromise authentication.

FIDO Alliance strongly supports the approach taken by the EBA here to determine whether something is an obstacle based not on the access model it implements, but rather the actual user experience. The example above (using OTP via SMS) would create the same issues with obstacles, delays and friction regardless of the model used – redirect, decoupled or embedded – making clear that the model used is not the primary cause of obstacles to a superior customer journey.

As an aside, we note that FIDO standards can be used to support user-friendly authentication via other envisioned models as well. FIDO is ideally suited to use in the decoupled model, for example, where an ASPSP asks the PSU to authenticate via the ASPSP's dedicated mobile app or any other application or device which is independent from the online banking frontend. Given the number of financial services firms building FIDO support into their mobile app, we expect this will an increasingly common approach in open banking going forward.

We note that FIDO authentication can be used in all models envisioned, however, there are aspects of the embedded model that may create security risks, given the need to share authentication keys between applications. On balance, implementation of FIDO with the redirect or decoupled models offers the best balance of security and user experience, delivering an excellent customer journey.

To that point: FIDO Alliance believes that the EBA's decision to not require that an ASPSP support multiple models for access is a sound one. If an ASPSP can deliver an excellent user experience through a single model – such as redirect using FIDO authentication – then that should suffice.

**Question 5: Do you agree with the EBA's assessments for design and testing, the options it considered and progressed or discarded, and the requirements proposed Guideline 6? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here. In particular, we appreciate the EBA's recognition that two different PSPs may define "satisfaction" in ways that are opposed to each other – creating a situation where one of them would be certain to get no satisfaction, no matter how hard an ASPSP tries. Given that, we believe the approach the EBA has taken here around design and testing is quite sensible.

**Question 6: Do you agree with the EBA's assessment for 'widely used', the options it considered and discarded, and the requirements proposed Guideline 7? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

**Question 7: Do you agree with the EBAs assessment to use the service level targets and statistical data for the assessment of resolving problems without undue delay, the options it discarded, and the requirements proposed Guideline 8? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

**Question 8: Do you agree with the proposed Guideline 9 and the information submitted to the EBA in the Assessment Form in the Annex? If not, please provide your reasoning.**

We believe the EBA has taken a reasonable approach here.

One concern amongst our members since the publication of the RTS has been that if the process for CA to exempt an ASPSP from developing a fallback option is too onerous, it would serve as a disincentive for that ASPSP to develop excellent API-based customer interfaces and instead incent ASPSPs to simply develop a fallback option. The impact of such an outcome would be to set back progress in migrating open financial services to one based on secure APIs.

By making it less onerous for a CA to issue a waiver, it in turn will incent ASPSPs to invest in high-quality API-based interfaces that are better for security, privacy and the customer journey.

**Question 9: Do you have any particular concerns regarding the envisaged timelines for ASPSPs to meet the requirements set out in these Guidelines prior to the September 2019 deadline, including providing the technical specifications and testing facilities in advance of the March 2019 deadline?**

We do not have any concerns.

**Question 10: Do you agree with the level of detail set out in the draft Guidelines as proposed in this Consultation Paper or would you have expected either more or less detailed requirements on a particular aspect? Please provide your reasoning.**

On balance, we agree with the level of detail. We believe it provides solid guidance to CAs – and industry at large – around how to proceed, without being overly prescriptive. Such an approach will allow innovation to flourish.

In contrast, an approach that seeks to micro-manage outcomes is likely to inhibit innovation and lock consumers and businesses in to models that are less than optimal. We appreciate the balanced approach that the EBA took here.

We greatly appreciate EBA's consideration of our comments. We look forward to further discussion with EBA on this topic, and would welcome the opportunity to answer any questions. Please contact our Executive Director, Brett McDowell, at brett@fidoalliance.org.