fido alliance | simpler stronger authentication

31 August, 2017

Member States' Financial Services Attachés
European Council

To Whom It May Concern:

I write to you today on behalf of the Fast IDentity Online Alliance (FIDO Alliance), a consortium of over 250 organizations from around the world collaborating to improve the state of online authentication by developing open technical standards and advocating industry best practices. We have been close observers of – and interested stakeholders in – the current discussions between the European Commission (EC) and European Banking Authority (EBA) around the Regulatory Technical Standard (RTS) for Strong Customer Authentication (SCA) under the Payment Services Directive 2 (PSD2). Specifically, we are writing in regards to the question of whether there should be a "fallback option" included in the RTS, allowing Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) to access consumer bank accounts through the legacy "user-facing interfaces" banks provide today for consumer login, i.e. "credential sharing" to enable what is often referred to as "screen scraping."

As background, our members include both banks and FinTech firms, as well as major payment card networks, health providers, mobile network operators, hardware manufacturers, software vendors and government agencies. Collectively, the FIDO Alliance represents the largest consortium in the world focused on authentication – with a specific focus on ensuring that authentication solutions preserve and enhance privacy.

FIDO Alliance has been active in the PSD2 discussion for quite some time, as evidenced by our January 2016 response to the EBA's Discussion Paper,[1] our March, 2016 executive briefing with EC Vice President Andrus Ansip,[2] our subsequent comments to the EBA on the draft RTS last October,[3] and the "Future of Authentication Policy Forum" we hosted in Brussels this past March.[4]

[1] See https://fidoalliance.org/resources/FIDO_EBA_Response_2016-02-08.pdf
[2] See https://twitter.com/EUintheUS/status/708024702778867713
[3] See https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2?p_p_auth=AuKmCnb9&p_p_id=169&p_p_lifecycle=0&p_p_state=maximized&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=2&_169_struts_action=%2Fdynamic_data_list_display%2Fview_record&_169_recordId=1616947
[4] See https://fidoalliance.org/events/future-of-authentication-forum

The EC was correct to flag Strong Customer Authentication as an essential component to enabling the vision of PSD2. The success of PSD2 is highly dependent on the use of Strong Customer Authentication solutions that are not only highly secure, but also easy to use, respectful of privacy, and built on open industry standards that enable interoperability across competing solutions and ultimately lead to lower costs of operation.

Against that backdrop, we have a number of observations regarding the current policy debate over whether the EBA should allow a "fallback option," for third-party account access, as detailed in the May 24, 2017 letter[5] from the EC, as well as the EBA's June 29 response.[6]

We write not only as experts in cybersecurity, identity, authentication and privacy – but also as experts in designing and deploying critical systems at scale that allow innovation to flourish while also protecting security and privacy. Our observations are as follows:

1. The most secure and efficient way for consumers to authorize third parties to access bank accounts today is through the use of Application Programming Interfaces (APIs), authorized by means of unphishable strong customer authentication, i.e. credentials based on public key cryptography as opposed to historic "shared secret" such as passwords and one-time-passcodes which are inherently vulnerable to phishing attacks. We believe the EBA did an admirable job in its approach to the RTS, by looking to embrace this industry-standard best practice for PSD2.

    - These API-based solutions have the added benefit of providing not just better security but also better privacy – as they allow consumers to grant access to their bank accounts on a granular level, choosing to share some details but not others.

    - They are based around proven global standards such as OAuth 2.0 and OpenID Connect (OIDC) that are trusted to manage access control for billions of user accounts.

    - When paired with FIDO standards for strong authentication, API-based solutions gain the benefits of device-based multi-factor authentication that is both safer and easy for consumers to use than typing codes into a form.

[5] See http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9

[6] See https://www.eba.europa.eu/documents/10180/1894900/EBA+Opinion+on+the+amended+text+of+the+RTS+on+SCA+and+CSC+%28EBA-Op-2017-09%29.pdf/df60c6ac-a284-4772-b1d5-66c7073d28af

2. Any approach that would allow the use of single-factor authentication via usernames and passwords as a "fallback option" is fundamentally at odds with language in the PSD2 requiring that customer authentication be "strong."

    - Passwords are, by far, the most commonly exploited attack vector in cyberspace today, accounting in 2016 for 81% of breaches worldwide.[7]

    - Breach after breach has made clear that there is no such thing as a "secure" or "strong" way to use passwords; between phishing, key-logging malware, brute force attacks, man in the middle attacks, thefts of password databases, and frequent password reuse across accounts, attackers have numerous tools at their disposal to compromise password-protected accounts. [8]

    - Even the most complex of passwords are routinely, compromised – most often by phishing attempts; there simply is no way to deliver strong security in today's environment through use of a password alone.

3. Any approach where consumers are asked to share their password with another entity puts consumers at increased risk.

    - Endorsing the practice of sharing passwords with 3rd party entities by establishing this as a normal and trusted pattern of behavior creates significant risk by training the user to be inherently more vulnerable to phishing attacks.

    - Assumptions that password databases can be adequately protected are simply not supported by history. Every year since FIDO Alliance first started tracking industry reports in 2013, data breaches of password credentials, which are

---

[7] See Verizon 2017 Data Breach Investigations Report (DBIR) http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[8] Note that in the United States, the Federal Financial Institutions Examination Council (FFIEC) issued an alert in 2016 flagging the importance of this issue for banks, noting: *Recent reports indicate an ongoing and increasing trend of attacks by cyber criminals to obtain large volumes of credentials. These attacks include theft of users' credentials—such as passwords, usernames, e-mail addresses—and other forms of identification used by customers, employees, and third parties to authenticate themselves to systems as well as theft of system credentials, such as certificates. User credentials can be stolen in many ways, including phishing and spear-phishing, malvertising, watering holes, and web-based attacks.*
Stolen credentials are often sold in cyber-criminal forums and then used to commit fraud through account takeovers and identity theft. Users may significantly increase exposure by creating usernames and passwords that are easy to guess or using the same usernames and passwords to access accounts on multiple Web sites. The theft of each type of user credential presents distinct risks. Stolen customer credentials may give an attacker access to customers' account information to commit fraud and identity theft. See FFIEC Joint Statement "Cyber Attacks Compromising Credentials" https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf

inherently valued targets for attack[9], has increased and is still on the rise because each large-scale breach enables yet more breaches through replay attacks using those same stolen credentials.[10]

4. Any approach where a third party can "log in as if they were a consumer" to a bank puts all parties at risk.

    - Such an approach is directly oppositional to bank efforts to deploy SCA based upon multi-factor authentication (MFA) to consumers – as most MFA solutions, by definition, lack a static component that can be shared with a third party. For example:

        - A one-time password changes every 30 to 60 seconds
        - Privacy-respecting biometrics reside with the consumer and are bound to their personal device; they cannot be copied and shared
        - Likewise, a FIDO cryptographic credential is designed to never be removed from the device that generated it

      Given these facts, a consumer choosing to use 3rd-party services under the proposed continued credential sharing methodology would first need to "turn off" their multi-factor SCA protections provided by their bank because that is the only way for a third party to log in with that consumer's password under this proposal. At a time when banks are looking to apply stronger forms of authentication to consumer accounts – and governments are encouraging or requiring them to do so – such a move undermines these efforts.

    - Credential sharing obviates the use of "Transaction Risk Analysis" solutions. Financial institutions, like most major online sites, generally look to use analytics to evaluate each login event and ascertain the likelihood that the login credential has been stolen or compromised. These analytics systems generally look at specific data points such as the location of the device, its IP address, data on the device itself, and other contextual data to evaluate risk. The value of these systems has been strong enough that the EBA itself has proposed allowing financial services firms to make use of "Transaction Risk Analysis" solutions in

[9] See https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html
[10] See https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

lieu of traditional, multi-factor authentication for transactions under a certain value.

However, the value of these systems are undermined when a login event is coming not from a consumer's device – but instead is coming from a third party who has obtained the password and is essentially "impersonating" the consumer. This undermines the security of the entire login system.

5. Any approach where consumers are asked by firms to hand over their username and password to their bank accounts directly contradicts the security advice government and industry give consumers around avoiding phishing attacks.

    - Up front, we note that phishing attacks are an increasing problem. The most recent data from the Anti-Phishing Working Group (APWG)[11] report, entitled "Phishing Attack Campaigns in 2016 Shatter All Previous Years' Records," noted that the total number of phishing attacks in 2016 was up by 65% over 2015. Phishing attacks on financial services accounted for 1 out of every 5 attacks. Thus, it is important that government be consistent in its messaging to consumers on best security practices such as "never share your password."

    - At a time when the security community is working[12] to[13] train[14] consumers[15] to safeguard[16] their credentials[17], approaches that ask consumers to share these credentials undermines the security of the online ecosystem.

In summary: we do not see any way in which the approach requested by the EC on May 24 can be implemented to the level of enhanced security called for in PSD2. Sharing passwords is simply a bad practice from a security perspective. It places banks, FinTech firms and their customers at increased risk – given the security vulnerabilities, the EC would be wise to not actively facilitate ongoing engagement in any scheme where passwords are shared. As we noted earlier, there are far more secure ways for consumers to delegate access to their bank accounts, involving APIs protected by strong customer authentication credentials.

That being said, we also note that we are aware of concerns that some Account Servicing Payment Service Providers (ASPSPs) will not be prepared to support SCA-compliant, API-based dedicated interfaces in time to comply with current PSD2 guidelines. While we support the

[11] See http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf
[12] See https://www.antiphishing.org//resources/Educate-Your-Customers/
[13] See https://www.paypal.com/us/webapps/mpp/brc/safety-and-security-phishing
[14] See https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx
[15] See https://www.financialfraudaction.org.uk/consumer/advice/protect-your-onlinemobile-banking/
[16] See https://auspost.com.au/about-us/about-our-site/online-security-scams-fraud/scam-alerts
[17] See https://www.consumer.ftc.gov/media/game-0011-phishing-scams

mission of the SCA requirements in PSD2 and we believe such requirements will improve the reliability of mobile commerce across Europe, we would not recommend introducing these new requirements ahead of the industry's ability to adequately prepare themselves as such an approach could be unnecessarily disruptive to existing commercial practices. Therefore, to the extent that the EC, after studying the readiness of ASPSPs, believes a "fallback option" needs to be supported to address any systemic gaps they discover, we suggest that this may be better addressed through a policy exemption to the RTS allowing for the use of this shared credential option for a limited time – perhaps 6-12 months – while ASPSPs bring their systems into compliance.

However, we do not believe it is appropriate to include such a provision in the RTS itself. The RTS, by its nature, is an important technical standard that will guide the market for years to come. As such, the RTS should focus on setting a high mark for SCA and common and secure communication under PSD2 – not articulate methods for stakeholders to avoid their responsibilities under this historic advancement in consumer protection policy. Inclusion of the "fallback option" in the RTS itself would dilute its message, undermine the intent of PSD2 and its requirements for SCA, and place consumers at increased risk.

We greatly appreciate your consideration of our views, and would be happy to confer further on this topic. Please let us know if we may be of assistance.

Sincerely,

Brett McDowell
Executive Director
The FIDO Alliance