Trustly

Ministry of Justice and Public Security
Postboks 8005 Dep,
0030 Oslo
Norway

Stockholm, 5 December 2017
Your ref: 17/4746 EP HEA/MEK/bj

HØRINGSSVAR – FORSLAG TIL NY FINANSAVTALELOV

1. INTRODUCTION

We refer to the consultation paper from the Ministry of Justice and Public Security (the "Ministry") dated 7 September 2017 regarding proposed amendments to the Norwegian Financial Contracts Act that would incorporate three EU directives including the Payment Services directive ("PSD2").

As a payment initiation services provider ("PISP") throughout the European Economic Area, Trustly has several comments to the proposed implementation in the Financial Contracts Act of the relevant sections in PSD2 concerning PISP.

2. SUMMARY

- The Ministry's view that contractual terms that require the user to not reveal BankID-information are not in themselves an obstacle to the provision of PIS and AIS, and therefore compliant with the requirements of PSD2, is incorrect.

- PSD2 Article 97 gives PISP the right to rely on the authentication methods made available by the account providers (banks) to their customers.

- The full harmonisation of the Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2) (the "SCA RTS") confirms the right of PISP to use those authentication methods that the banks provide and the draft RTS establishes the security requirements for the handling of user personalized security credentials ("PSC").

- A revised draft of the Financial Contracts Act must reflect the requirements of PSD2 and implement the SCA RTS (adopted as a regulation) and avoid the possibility of any ambiguity that might be exploited by account providers.

Trustly

3. THE PAYERS' RIGHT TO MAKE USE OF PAYMENT INITIATION SERVICES

3.1. Current view of the Ministry

Section 4.5.2 of the consultation paper discusses the customers' right to enter into agreements for payment initiation services ("PIS") in accordance with PSD2 Article 66 (1):

> *Article 66*
> *Rules on access to payment account in the case of payment initiation services*
> *1. Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online.* (Emphasis added.)

The consultation rightly points out that in order to be able to provide PIS the provider needs to be able to access the payer's account. PIS involves establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider (the bank account provider) in order to initiate internet payments on the basis of a credit transfer. Access to the payer's account requires the use of the authentication procedure provided by the bank and PSD2 therefore contains an obligation for the PISP to safeguard the PSC it receives:

> *Article 66*
> *3. The payment initiation service provider shall:*
> *(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;* (Emphasis added.)

The consultation paper concludes, correctly, in our view, that the directive entails that the member states must ensure the users' right to use PIS, and that this right is not obstructed in the terms and conditions found in the agreements between the customer and the account servicing payment service provider.

However, Trustly does not agree with the stated view of the Ministry that it would not be considered obstruction to permit Norwegian banks to refuse to let their customers use the most common method for authentication, BankID, as long as they provide an alternative authentication method.

> "*It is, for the time being, the view of the Ministry*[1] *that contractual terms that require the user to not reveal BankID-information are not in themselves an obstacle to the provision of PIS and AIS. Whether such terms are an obstacle and violate the directive will depend on whether the account servicing payment service provider can arrange another way in which the user can efficiently make use of their right to such services. The Ministry points out that such accommodation cannot demand any other requirements to the PIS/AIS providers other than those contained in the directive.* " (Unofficial translation – emphasis added)

This view of the Norwegian Ministry of Justice and Public Security is not directly reflected in the proposed wording for the new Financial Contracts Act, however, the proposed text does not give PISP and AISP a specific right to use all means of authentication issued by the Banks. Furthermore, the obligation of the account holder to protect any PSC it receives[2] when seen in

[1] Ministry of Justice and Public Security

[2] article 57 of the proposed Financial Contracts Act

conjunction with the stated understanding of the Ministry in the consultation paper means that Norwegian banks may continue to discriminate against PIS such as Trustly in the provision of PIS/AIS services based on the current proposal.

BankID is used by all Norwegian banks to give customers access to their online banking solutions and to use payment cards issued by the banks and has more than 3.7 million users. Denying PISP/AISP access to this authentication method would result in a significant competitive disadvantage for providers of PIS and AIS outside of the traditional account provider (banking) system and would not be in compliance with PSD2 as discussed further below.

The apparent reason given for the Ministry's decision to adopt this understanding of PSD2 is that:

> *"... some of the Norwegian solutions for logging on to internet banks happens via a mechanism that can be described as the user's "master key" – it gives full access to the internet bank and a number of public services. It would therefore be unfortunate if this "master key" was made available to a PISP or AISP. A solution could therefore be that the account servicing payment service provider equip the user with a "guest key" with limited functionality, and which can be given to the PISP or AISP."*

The understanding of the Ministry is based on an incorrect premise about security risks related to PISP and AISP. Furthermore the Ministry's understanding and proposed solution is not compliant with the requirements of PSD2.

3.2. Unsubstantiated security claims

3.2.1 PIS has an exceptional security track record

The apparent decision by the Ministry to permit banks to discriminate against PISP and AISP appears to be founded on claims that such transactions are unsecure. However, the use by a customer of a third party to initiate a payment from his/her account (PIS), is not an unsecure and unproven concept.

Trustly is a licensed Payment Institution under the supervision of the Swedish Financial Supervisory Authority operating in 29 countries and communicates 3.2 million transactions per month. Trustly already provides its services in Sweden and Denmark based on the customers using the equivalent of BankID in those countries. The market leader in Europe for this type of payment service operates in 13 countries and communicates over 5 million transactions per month. Neither Trustly nor, to Trustly's knowledge, any other PISP have ever had any instance of data fraud.

Even though PIS are currently being provided in a secure and efficient manner outside of the regulatory framework of the current payment services directive, the introduction of PSD2 will bring PIS under regulation and lead to increased protections for customers and make payment services even safer and more resilient. Firms providing payment initiation services will need to apply for authorisation and as part of the authorisation process firms will need to demonstrate that they have implemented effective security systems and controls, access to sensitive payment data, incident management and business continuity.[3] PISP will i.a. need to:

[3] Final Report on the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers

- provide security policies and procedures, including a risk assessment in relation to their services, and describe security controls and mitigation measures designed to protect payment service users
- demonstrate that they have effective processes to monitor and handle incidents and security-related customer complaints
- have established plans for how to deal with significant continuity disruptions, such as the failure of key systems, the loss of key data, or lack of access to premises
- demonstrate that they have an effective process to file, monitor, track, and restrict access to sensitive payment data such as data classification, access management, and monitoring tools

The notion that PISP are unreliable or not serious actors in the payment services industry and that *"[i]t would therefore be unfortunate if this "master key" was made available to a PISP"* is highly incorrect.

The claimed security concerns relating to PIS have historically been promulgated by financial institutions with a vested interest in limiting competition in the payment services market, but are not based on any factual data. In its dialogue with Bank ID Norge and Finance Norway Trustly has requested more precise information on their security concerns, but such concerns remain vague assertions.

Similar security claims against PISP have previously been made by the German banks via their central association "Deutsche Kreditwirtschaft" to justify terms and conditions that would have prohibited their customers from using PIS services. However, the German Federal Cartel Office found that such terms restricted competition and rejected security concerns brought forward as a means of justification. The banks were unable to demonstrate the alleged security risks and it was concluded that no specific cases of abuse were known. [4]

3.2.2 Authentication codes as a "master key"

We would also like to point out that it is not accurate to describe the PSC that a PISP may receive in its communications as being given access to a "master key" that would give full access to the internet bank of a user and also their personal profiles with a number of public services.

BankID generates authentication codes that can only be used one time and for BankID on mobile there is also a "dynamic linking" element so that the authentication code generated is specific to the amount of the payment transaction. Accordingly, access by PISP to an individual authentication code does not give it full access to any other services that BankID might be used for and with dynamic linking any possibility of interfering with payment information during each individual transmission is also eliminated. Moreover, in relation to BankID on mobile no credentials will pass through the PISP, thus, eliminating any concern of a "master key" being shared with the PISP.

Under PSD2 the EBA, as subscribed to by the European Commission's adoption 27 November 2017 of the final version in a regulation, has in the SCA RTS developed a principle-based approach with requirements to protect confidentiality and integrity in the creation, association with PSUs, delivery, renewal and destruction of PSCs[5]. This includes the use of one off codes and

[4] Section III, Summary of the Opinion of the Federal Cartel Office in the Court procedure giropay ./. Payment Network (File number 84 O 2/10, District Court of Cologne)

[5] SCA RTS Chapter IV
http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

dynamic linking. Under PSD2 dynamic linking must be used for the authentication of all electronic remote payment transactions such as when using PIS[6] further ensuring the security for customers of using PIS.

3.2.3 Authentication to banking and public services

The comments from the Ministry can be understood such that they consider the Norwegian authentication solutions that can provide access to both internet banking and public services as unique and requiring special considerations with regard to PSC safety requirements.

While it is correct that Norway is ahead of most other European countries with regard to authentication procedures, we would like to point out that regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) aims to enable secure and seamless electronic interactions between businesses, citizens and public authorities and ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. However eIDs are not intended just for accessing online public services, and the European Commission's Consumer Financial Services Action Plan makes it clear that the eID scheme is also intended for financial services and online business[7].

3.3. Authentication under PSD2

Under PSD2 Article 36 payment institutions shall have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis and such access shall be sufficiently extensive as to allow payment institutions to provide payment services in an unhindered and efficient manner. Furthermore , under PSD2 Article 97(5), AISP and PISP have a right to rely on all the authentication procedures provided by the account servicing payment service providers to their users.

> *Article 97*
>
> ***Authentication***
>
> *1. Member States shall ensure that a payment service provider applies strong customer authentication where the payer:*
> *(a) accesses its payment account online;*
> *(b) initiates an electronic payment transaction;*
> *(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*
>
> *2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.*
>
> *3. With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.*

---

[6] PSD2 Article 97(2)

[7] " Financial services, but also other sectors (e.g. online platforms), have a huge opportunity to seize by providing or relying on eIDs which will enable their customers to do business online across all EU Member States." https://ec.europa.eu/futurium/en/blog/accelerating-uptake-eidas-update

> *4. Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.*
>
> *5. Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.* (Emphasis added.)

The understanding of the Ministry that banks may include contractual terms that would prevent AISP and PISP from using certain authentication procedures is not compatible with this right. This even seems to be acknowledged by the Ministry when they state on page 72 of the consultation paper:

> *"In Denmark they have proposed a rule that "the account servicing payment services provider shall give PIS providers and AIS providers permission to use the authentication procedures that the account servicing payment services provider makes available for its users". In this is an implicit requirement that the account servicing payment services provider cannot prevent the AISP/PISP from getting access to authentication procedures"* (Emphasis added.)

It is possible that the Ministry was of the understanding that the rule proposed in Denmark was a clarification in the national implementation of PSD2, but it is just implementing article 97(5).

Article 97(5) does place certain conditions on the access by PISP to the banks' authentication procedures when stating that it must be in accordance with article 97 paragraphs 1, 2 and 3. The authentication procedure must be based on strong customer authentication where the payer initiates an electronic payment (paragraph 1), for electronic remote payment transactions, the strong customer authentication must include elements which dynamically link the transaction to a specific amount and a specific payee (paragraph 2) and payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials (paragraph 3).

Moreover, PSD2 Article 68(5) regulates that situations in which an ASPSP can deny a PISP access to a payment account.

> *Article* 68
> ***Limits of the use of the payment instrument and of the access to payment accounts by payment service providers***
> *5. An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction.* (Emphasis added.)
>
> *6. In the cases referred to in paragraph 5, the account servicing payment service provider shall immediately report the incident relating to the account information service provider or the payment initiation service provider to the competent authority.*

Trustly

In accordance with Article 68(5) an ASPSP has very limited possibilities to deny a PISP access to a payment account. The situations regulated in Article 68 relate to unauthorised or fraudulent use by a PISP. By including a possibility for the ASPSP to deny access to a payment account by virtue of contractual terms relating to BankID the Ministry has extended the possibility an ASPSP has to deny access to a payment account beyond that of PSD2, which is in clear violation of the intent and purpose of PSD2. That the Ministry goes beyond the intention and purpose of PSD2 is clear when taking the Ministry's position and Article 68(5) into account. It will, pursuant to Article 68(6), be required for the ASPSP to notify the competent authority each and every time a user accepts the BankID contractual terms as PISPs will be denied access to the payment account due to the contractual terms. Considering that thousands of users will be covered by the BankID contractual terms the competent authority will receive, and have to deal with, thousands of such notifications, which obviously is not the intention of PSD2.

PSD2 Article 98 requires the EBA to draft regulatory technical standards (RTS) that specify the requirements of the strong customer authentication and security measures referred to in article 97 paragraphs 1, 2 and 3. A final report with draft RTS on Strong Customer Authentication and common and secure communication under PSD2 Article 98 was published on 23 February 2017. The European Commission adopted the SCA RTS on 27 November 2017 by way of a regulation (full harmonisation), and it contains, along with the related discussion and consultation papers further information and discussion specifically related to the issue of PISP access to PSCs. The SCA RTS is due to become applicable around September 2019, 18 months after the date of entry into force of the SCA RTS.

The SCA RTS reiterates the right that PIS have to make use of the authentication procedures provided by that banks in Article 30 (2) and that the ASPSP cannot require additional authorisations or additional checks of the consent provided by the user to the PISP in Article 32(3)

> *Article 30*
> ***General obligations for access interfaces***
> *2. For the purposes of authentication of the payment service user, the interfaces referred to in paragraph 1 shall allow account information service providers and payment initiation service providers to rely on* ***all*** *the authentication procedures provided by the account servicing payment service provider to the payment service user.* (Emphasis added.)

> *Article 32*
> ***Obligations for a dedicated interface***
> *3. Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.*

The SCA RTS also contains specific requirements for common and secure open standards of communication. Throughout the legislative process for the RTS the question of protecting users PSC's was a central issue and the EBA invited comments and posed questions in their discussion

paper published 8 December 2015 [8] and consultation paper published 12 August 2016[9] related to the protection of PSC's.

The EBA points out in the discussion paper that the primary method for ensuring the security of PSCs is by bringing PISP in the scope of regulated entities. The EBA is explicit in pointing out that the consequence of regulating PIS is not just that PISP will be subject to a number of security measures, but also that his means that PISP can rely on all the authentication procedures provided by the account providers:

> *55. This development [PIS and AIS] has increasingly lead to PSUs accessing the online facility of their ASPSPs payment account via the IT infrastructure of a third party provider, involving the transmission or storage of the PSU's PSC. In order to achieve the aim expressed in recital 33 PSD2, which is to ensure continuity in the market, by enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework, the PSD2 brings AIS and PIS providers in the scope of regulated entities*
>
> *57. Inclusion of the AIS and PIS services under PSD2 has in particular the following consequences for market participants:*
>
> *ii. Regulated PSPs, including AIS, PIS providers will have to comply with all the security measures deriving from the PSD2 (title IV) and delegated acts (title V). As explained in the background section, it is important to underline that only 18 months after their adoption by the Commission, will PSPs have to comply with the Regulatory Technical Standards on strong customer authentication and secure communication.*
>
> *v. AIS and PIS providers will be able to rely on the authentication procedures provided by the ASPSP to the PSU to provide their services (Article 97.5). Recital 30 outlines in particular that "the personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers". (Emphasis added.)*

Subsequently in the EBA consultation paper the EBA again made their understanding of PIS use of authentication procedures clear.

> *19. In relation to how Article 97(1)b should be applied by PSPs for a card payment transaction or the provision of PIS, the EBA understands that:*
> *a) in accordance with Article 97(5), PISPs have the right to rely on the authentication procedures provided by the account servicing payment service provider (ASPSP) to the user. In such cases, the authentication procedure will remain fully in the sphere of competence of the ASPSP.*

---

[8] Sections 4.3 and 4.4 Questions 10-15 and related comments. EBA/DP/2015/03 8 December 2015 Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2). https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf

[9] Section 3.2.2/Question 6 and related comments. EBA-CP-2016-11 12 August 2016 Consultation Paper On the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2. https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf

68. In order to fulfil the mandate conferred on EBA by PSD2, which is to specify the requirement for secure communication between the relevant actors while remaining technologically neutral, the EBA has arrived at the view that the future RTS must not prescribe the use of a specific industry standard of internet communication. Instead, EBA proposes in the draft RTS the requirements with which every communication solution used for secure communication between ASPSPs, PISPs, AISPs, and PSPs issuing card-based payment instruments will have to comply for the provision of a payment service.

69. These requirements can be summarised as follows:

b) ASPSPs shall ensure that their communication interface allow PISP or AISP to rely on the authentication procedures provided by the ASPSP to the payment service user, in compliance with Articles 97(5), 66(3)b and 67(2)b of PSD2;

The EBA did receive a number of responses to the discussion Paper and the consultation paper with comments from banks on the access to the PSCs by AIS and PIS providers, however these comments were rejected by the EBA based on the security requirements that PSD2 and the RTS put in place. We refer to the comments section of the final report[10]:

Comments	**Summary of responses received**	***EBA analysis***	***Amendments***
[94] Chapter 3 (now Chapter 4)	Respondents expressed their disagreement with the AISPs/PISPs accessing personalised security credentials (PSC).	*Recital 30 PSD2, Article 66(3) and 67(2) PSD2 allow AISPs and PISPs to access and use PSCs and impose security requirements on these providers when transmitting the data.*	*None*
[281] General responses	*One respondent expressed concern about the high risk of phishing claims and was of the view that PSUs should only be allowed to enter their personalised security credentials received from their ASPSP in the secure internet environment of the ASPSP.*	*Article 97(5) PSD2 enables PISPs/AISPs to rely on authentication procedures of the ASPSP. This can therefore mean that PSC could be entered on a different website from the ASPSPs' website. The EBA is therefore of the view that any restriction as suggested by the respondent would be in breach of PSD2 and therefore cannot be accommodated.*	*None*

On the other hand there were some responses from PISP/AISP seeking additional clarity that the account providers and PISP/AISP should use the same authentication procedures in order to ensure neutrality and provide a level playing field between independent service providers and the banks.

"The exact same restrictions should apply to both independent AIS and ASPSP providing AIS to the PSU:

[10] Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf

- Same PSC. That is, the same user id and password for the ASPSP AIS (the electronic banking) than for any independent AIS. This would impede other passwords being revoked while the online banking can be accessed.[11]"

In their response the EBA points out that PSD2 already allows AISPs and PISPs to rely on the ASPSP's PSC:

[175] Article 19 (1)(c) (now Article 27(1))	*The respondents asked for authentication procedures to use the same PSC for independent AISP as for direct online access to the payment accounts.*	*The RTS do not prescribe PSC but PSD2 does allow AISPs and PISPs to rely on the ASPSP's PSC.*	*None*

3.4. Conclusions

In accordance with PSD2 and the SCA RTS, the revised Norwegian Financial Contracts Act must clearly state that account information service providers and payment initiation service providers can rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.

This requirement implies that the account servicing payment services provider cannot prevent the AISP/PISP from getting access to authentication procedures offered to their users, including BankID. PSD2 does not allow for banks to create a two-tiered system for authentication procedures.

Best regards,

Oscar Berglund,
CEO Trustly Group AB

[11] Identical consultation responses from Mooverang and Finect
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=uy1W7oVC&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=1615310